



Installation Guide for Cisco Unity Voice Messaging with Microsoft Exchange 2003/2000 (With Failover Configured)

Release 4.0(5) and Later
Revised March 9, 2006

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Installation Guide for Cisco Unity 4.0(5) and Later Voice Messaging with Microsoft Exchange 2003/2000 (With Failover Configured)

© 2006 Cisco Systems, Inc. All rights reserved.



Preface ix

Audience and Use	ix
Documentation Conventions	ix
Cisco Unity Documentation	xiii
Obtaining Documentation	xiii
Cisco.com	xiii
Product Documentation DVD	xiv
Ordering Documentation	xiv
Documentation Feedback	xiv
Cisco Product Security Overview	xiv
Reporting Security Problems in Cisco Products	xv
Obtaining Technical Assistance	xv
Cisco Technical Support & Documentation Website	xvi
Submitting a Service Request	xvi
Definitions of Service Request Severity	xvi
Obtaining Additional Publications and Information	xvii

CHAPTER 1

Overview of Mandatory Tasks for Installing Cisco Unity 1-1

Part 1: Installing and Configuring the Cisco Unity Server	1-1
Part 2: Installing the Secondary Server for Cisco Unity Failover	1-3
Part 3: Populating the Cisco Unity System with Subscriber and Call Management Data	1-4
Part 4: Configuring Failover and Setting Up Networking Options (If Applicable)	1-6
Part 5: Customizing the Cisco Unity Conversation	1-6
Part 6: Backing Up Cisco Unity	1-7
Part 7: Training	1-7

CHAPTER 2

Preparing for the Installation 2-1

Gathering Documentation and Tools	2-1
Downloading Software for the Installation	2-2
Software for All Installations	2-3
Additional Software for Installations with Cisco Unity DVDs or CDs Earlier Than the Currently Shipping Version	2-4
Determining the Drive Locations for Files on the Cisco Unity Server	2-4

Drive Locations for Files on a Platform Overlay 1 Server	2-5
Drive Locations for Files on a Platform Overlay 2 Server	2-5
Drive Locations for Files on a Platform Overlay 3 Server	2-6

CHAPTER 3

Setting Up the Hardware 3-1

Installing Voice Cards	3-1
Attaching Peripheral Devices and Making Connections from the Phone System	3-5

CHAPTER 4

Installing the Operating System 4-1

Configuring the RAID Arrays	4-1
Using the Cisco-Provided Array-Configuration Utility	4-2
Using the Manufacturer-Provided Array-Configuration Utility	4-3
Installing Windows Server 2003 or Windows 2000 Server	4-3
Windows Server 2003: Using the Manufacturer's Guided System-Setup Utility and a Retail Windows Server 2003 Disc	4-4
Windows 2000 Server: Using the Cisco Unity Platform Configuration Discs	4-5
Windows 2000 Server: Using the Manufacturer's Guided System-Setup Utility and a Retail Windows 2000 Server Disc	4-7
Enabling Windows Terminal Services (Windows Server 2003 Only)	4-9
Setting Up the Logical Drives	4-9

CHAPTER 5

Customizing the Cisco Unity Platform 5-1

Configuring a Dual NIC in the Cisco Unity Server	5-2
Installing the NIC-Configuration Utility	5-2
Configuring a Dual NIC	5-4
Obtaining Cisco Unity License Files	5-4
Running the Cisco Unity System Preparation Assistant	5-6
Changing Folder Settings in Windows Explorer	5-8
Installing the Latest Microsoft Service Packs and Updates for Windows, Internet Explorer, and SQL Server 2000	5-9
Disabling the Found New Hardware Wizard for the Voice Cards	5-10
Installing Virus-Scanning Software (Optional)	5-10
Installing and Configuring Cisco Security Agent for Cisco Unity (Optional)	5-11
Connecting the Cisco Unity Server to the Network	5-11
Configuring TCP/IP Properties	5-11
Verifying the IP Address and the Network Connection	5-12
Disabling Virus-Scanning and Cisco Security Agent Services	5-12
Adding the Cisco Unity Server to an Existing Domain	5-13

Resetting the Account That SQL Server Services Log On As 5-14

CHAPTER 6

Setting Up Exchange 6-1

Determining the Partner Exchange Server 6-2

Installing Exchange Administration Software on the Cisco Unity Server 6-2

 Installing Exchange 2003 Administration Software 6-2

 Installing Exchange 2000 Administration Software 6-4

Installing the Latest Exchange Service Pack and Updates 6-5

Extending the Active Directory Schema for Cisco Unity 6-6

Creating Organizational Units and a Mailbox Store 6-7

CHAPTER 7

Creating Accounts for the Installation and Setting Rights and Permissions 7-1

About the Accounts Required for the Cisco Unity Installation 7-2

 The Account Used to Install Cisco Unity 7-2

 The Account Used to Access the Cisco Unity Administrator 7-2

 The Accounts That Cisco Unity Services Log On As 7-2

Creating the Accounts Required for the Cisco Unity Installation 7-3

Adding the Cisco Unity Administration Account to the Local Administrators Group 7-3

Setting Rights and Permissions with the Cisco Unity Permissions Wizard 7-4

Setting Required Exchange Permissions 7-8

CHAPTER 8

Installing and Configuring Cisco Unity Software 8-1

Determining Whether to Set Up Cisco Unity to Use SSL 8-2

Installing the Microsoft Certificate Services Component 8-3

Installing and Configuring Cisco Unity Software 8-3

 Starting the Cisco Unity Installation and Configuration Assistant and Installing Cisco Unity Software 8-4

 Installing License Files 8-6

 Configuring Services 8-7

 Configuring Cisco Unity for the Message Store 8-8

 Setting New Default Passwords 8-9

 Integrating the Phone System with Cisco Unity 8-10

 Setting Up the Cisco Personal Communications Assistant to Use SSL 8-10

Installing the Cisco Unity Service Release, If Available 8-16

Testing the Phone System Integration 8-16

Excluding from Virus Scanning the Directory in Which Cisco Unity Is Installed 8-16

Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL 8-17

Securing the Example Administrator Account Against Toll Fraud 8-18
 Moving the Data Store Databases and Transaction Logs 8-18
 Re-enabling Virus-Scanning and Cisco Security Agent Services 8-21
 Securing Cisco Unity and the Cisco Unity Server 8-21

CHAPTER 9

Installing Optional Software 9-1

Installing RSA SecurID 9-1
 Installing Symantec pcAnywhere 9-1
 Recommended Configuration for pcAnywhere 9-2
 Installing Other Optional Software 9-3

CHAPTER 10

Setting Up Authentication for the Cisco Unity Administrator 10-1

Determining the Authentication Method to Use for the Cisco Unity Administrator 10-1
 Authentication Methods Available for the Cisco Unity Administrator 10-2
 How Integrated Windows Authentication Works with the Cisco Unity Administrator 10-3
 How Anonymous Authentication Works with the Cisco Unity Administrator 10-4
 Configuring IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication 10-5

APPENDIX A

Voice Cards and PIMG Units A-1

Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro A-1
 Hardware Settings A-2
 Intel Dialogic D/120JCT-LS and D/120JCT-Euro A-4
 Hardware Settings A-6
 Software Settings A-7
 Intel Dialogic D/240PCI-T1 A-8
 Hardware Settings A-9
 Software Settings A-10
 Intel NetStructure PBX-IP Media Gateway (PIMG) A-11
 Software Settings A-12
 Removing Intel Dialogic Voice Card Software A-12
 Determining the Current Settings for the Quiet Parameter and Other Parameters A-12
 Removing the Intel Dialogic Voice Card Software A-13
 Resetting the Quiet Parameter and Other Parameters A-14

APPENDIX B

Exiting and Starting the Cisco Unity Software and Server B-1

Exiting the Cisco Unity Software B-1
 Shutting Down or Restarting the Cisco Unity Server B-2

Starting the Cisco Unity Software B-3

APPENDIX C**Manual Installation Procedures for Software Installed by the Cisco Unity System Preparation Assistant During a New Installation C-1**

Installing MSXML 3.0 with Service Pack 1 C-1

Installing Windows Terminal Services C-2

Installing the NNTP Service C-2

Installing Message Queuing Services 2.0 C-2

Installing Windows 2000 Service Pack 4 C-3

Installing Internet Explorer 6.0 with Service Pack 1 C-3

Installing SQL Server 2000 and Service Pack 3a C-4

Installing the Microsoft .NET Framework C-5

INDEX



Preface

This preface contains the following sections:

- [Audience and Use, page ix](#)
- [Documentation Conventions, page ix](#)
- [Cisco Unity Documentation, page xiii](#)
- [Obtaining Documentation, page xiii](#)
- [Documentation Feedback, page xiv](#)
- [Cisco Product Security Overview, page xiv](#)
- [Obtaining Technical Assistance, page xv](#)
- [Obtaining Additional Publications and Information, page xvii](#)

Audience and Use

The Cisco Unity installation guide is intended for installers of a Cisco Unity system. You need a working knowledge of Microsoft Exchange 2003 or Exchange 2000, and Microsoft Windows 2003 or Windows 2000, depending on the versions you plan to use.

Documentation Conventions

Table 1 Cisco Unity installation guide Conventions

Convention	Description
boldfaced text	Boldfaced text is used for: <ul style="list-style-type: none">• Key and button names. (Example: Click OK.)• Information that you enter. (Example: Enter Administrator in the User Name box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter ping <IP address> .)

Table 1 Cisco Unity installation guide Conventions (continued)

Convention	Description
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press Ctrl-Alt-Delete .)
> (right angle bracket)	A right angle bracket is used to separate selections that you make: <ul style="list-style-type: none"> On menus. (Example: On the Windows Start menu, click Settings > Control Panel > Phone and Modem Options.) In the navigation bar of the Cisco Unity Administrator. (Example: Go to the System > Configuration > Settings page.)

The Cisco Unity installation guide also uses the following conventions:

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS**Waarschuwing****BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus	<p>TÄRKEITÄ TURVALLISUUSOHJEITA</p> <p>Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.</p> <p>SÄILYTÄ NÄMÄ OHJEET</p>
Attention	<p>IMPORTANTES INFORMATIONS DE SÉCURITÉ</p> <p>Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.</p> <p>CONSERVEZ CES INFORMATIONS</p>
Warnung	<p>WICHTIGE SICHERHEITSHINWEISE</p> <p>Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.</p> <p>BEWAHREN SIE DIESE HINWEISE GUT AUF.</p>
Avvertenza	<p>IMPORTANTI ISTRUZIONI SULLA SICUREZZA</p> <p>Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.</p> <p>CONSERVARE QUESTE ISTRUZIONI</p>
Advarsel	<p>VIKTIGE SIKKERHETSINSTRUKSJONER</p> <p>Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.</p> <p>TA VARE PÅ DISSE INSTRUKSJONENE</p>

Aviso INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES**¡Advertencia! INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES**Varning! VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR**Figyelem FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmeztető jel veszélyre utal. Sérülésveszélyt rejte helyzetben van. Mielőtt bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplő figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján kereshető meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!**Предупреждение ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告**重要的安全性说明**

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告**安全上の重要な注意事項**

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

Cisco Unity Documentation

For descriptions and URLs of Cisco Unity documentation on Cisco.com, refer to the *Cisco Unity Documentation Guide*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmap09186a00801179df.html.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



Overview of Mandatory Tasks for Installing Cisco Unity



Note

If you are upgrading Cisco Unity, refer instead to the *Cisco Unity Reconfiguration and Upgrade Guide* for upgrade instructions.

Use the following high-level task list to install the Cisco Unity system correctly. The tasks reference detailed instructions in the Cisco Unity installation guide, and in other Cisco Unity documentation as noted. Follow the documentation for a successful installation.

The task list leads you through the complete installation of the Cisco Unity system—from installing and configuring the Cisco Unity server; to populating the Cisco Unity system with subscriber and call management data; to setting up optional features, such as failover and networking; to backing up Cisco Unity.



Note

Cisco assumes that the Exchange environment is already set up and working before the Cisco Unity system is installed.

The list is divided into seven parts. Some of the tasks apply only to specific situations, and are noted as such. If a task does not apply to your situation, skip it.

We recommend that you check off tasks as you complete them.

Part 1: Installing and Configuring the Cisco Unity Server

The tasks in Part 1 reference chapters in the Cisco Unity installation guide, unless otherwise noted.



Note

Begin the installation on the computer that will be the primary Cisco Unity server. The task list alerts you when to install the secondary Cisco Unity server. Both servers must have the same enabled features and configurations.

1. Confirm that you are using the correct version of the Cisco Unity installation guide for your configuration. This version of the guide is for Cisco Unity 4.0(5) and later Voice Messaging with Exchange 2003 or Exchange 2000, configured for failover. For a list of configurations and applicable installation guides, refer to the document *Use the Installation Guide That Matches the*

Cisco Unity 4.0(5) or Later Configuration at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guide09186a008042173f.html.

2. Verify the following requirements:
 - a. System requirements for the Cisco Unity 4.x system, including requirements for the failover feature. Refer to the applicable version of *Cisco Unity System Requirements* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
 - b. Requirements for integrating the phone system(s), including requirements for the failover feature. Refer to the “Requirements” section of the applicable Cisco Unity integration guide(s) at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.
 - c. *If the system is using Cisco Unity Bridge Networking*: Requirements for the Bridge. Refer to the applicable version of *Cisco Unity Bridge System Requirements, and Supported Hardware and Software* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
 - d. *If the system is using any Cisco Unity networking option (including the Bridge)*: Requirements for the networking option. Refer to *Cisco Unity Networking Options Requirements* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_table09186a0080531ba9.html.
3. Gather the documentation and tools for the installation, download the latest Microsoft updates and other software, and determine the drive locations for application, log, and database files that you will need later in the installation. See the “[Preparing for the Installation](#)” chapter.
4. Set up or program the phone system(s) and extensions to enable the integration(s) with Cisco Unity. Refer to the “Programming the <Name> Phone System” section of the applicable Cisco Unity integration guide(s) at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.
5. Set up the Cisco Unity server, install voice cards and attach peripheral devices, if applicable, and make connections from the phone system. See the “[Setting Up the Hardware](#)” chapter.
6. Configure the RAID arrays, if applicable, install Windows Server 2003 or Windows 2000 Server, and create the logical drives, if applicable. See the “[Installing the Operating System](#)” chapter.
7. Obtain Cisco Unity license files, and use the Cisco Unity System Preparation Assistant to configure the operating system and install required software components. Then set up the server in the Windows networking environment. See the “[Customizing the Cisco Unity Platform](#)” chapter.
8. Install and configure the applicable Exchange software. See the “[Setting Up Exchange](#)” chapter.
9. Create the accounts required for the Cisco Unity installation, and set rights and permissions. See the “[Creating Accounts for the Installation and Setting Rights and Permissions](#)” chapter.
10. Decide whether to set up Cisco Unity to use SSL and install the Microsoft Certificate Services component, if applicable, then use the Cisco Unity Installation and Configuration Assistant to install and configure Cisco Unity software, and to set up the Cisco Personal Communications Assistant to use SSL, if applicable. You also set up the Cisco Unity Administrator and the Status Monitor to use SSL, if applicable, then secure the Example Administrator account against toll fraud, and move SQL Server database files and transaction logs, if applicable. See the “[Installing and Configuring Cisco Unity Software](#)” chapter.

11. Install any optional software. See the “Installing Optional Software” chapter.



Caution Do not install Microsoft Outlook on the Cisco Unity server, or Cisco Unity may not notify subscribers of new messages.

12. Create an emergency repair disk that can be used to repair and restart Windows, if it is damaged. Refer to Windows Help.
13. Determine the authentication method that you want to use for the Cisco Unity Administrator web application, and configure IIS, as applicable. See the “Setting Up Authentication for the Cisco Unity Administrator” chapter.

Part 2: Installing the Secondary Server for Cisco Unity Failover

The tasks in Part 2 reference chapters in the Cisco Unity installation guide, unless otherwise noted.

14. *With a Cisco CallManager integration only:* On the phone system, add the voice messaging ports that will be used by the secondary server. Refer to the “Programming the Cisco CallManager Phone System” section of the applicable Cisco CallManager integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.
15. On the secondary server, repeat the following Part 1 tasks, depending on the phone system integration being used:
 - For Cisco CallManager, repeat Task 6. through Task 8.
 - For a circuit-switched phone system, repeat Task 5. through Task 8.
16. For the same accounts that you created in Task 9., add the Cisco Unity administration account to the local Administrators group, and run the Cisco Unity Permissions wizard to set rights and permissions. See the “Creating Accounts for the Installation and Setting Rights and Permissions” chapter.
17. Use the Cisco Unity Installation and Configuration Assistant to install and configure Cisco Unity software, and to set up the Cisco PCA to use SSL, if applicable. You also set up the Cisco Unity Administrator and the Status Monitor to use SSL, if applicable, and move SQL Server database files and transaction logs, if applicable. See the “Installing and Configuring Cisco Unity Software” chapter.
18. Install any optional software. See the “Installing Optional Software” chapter.
19. Create an emergency repair disk that can be used to repair and restart Windows, if it is damaged. Refer to Windows Help.
20. Configure IIS so that the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, if you decided to use that method. See the “Setting Up Authentication for the Cisco Unity Administrator” chapter.
21. Store all of the software that was shipped with Cisco Unity together in a location that is safe and can be readily accessed. You may need the discs later to upgrade or to otherwise modify the Cisco Unity system, or Cisco TAC may require you to access them during a service call.

Part 3: Populating the Cisco Unity System with Subscriber and Call Management Data

You do most of the tasks in Part 3 by using the Cisco Unity Administrator. (For information on logging on to the Cisco Unity Administrator and on using it, refer to the “Accessing the Cisco Unity Administrator” chapter of the *Cisco Unity System Administration Guide*.)

The tasks reference chapters in the *Cisco Unity System Administration Guide, Release 4.0(5)* that contain detailed information; the guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_administration_guide_book09186a008043ea39.html.



Note

Do these tasks on the primary Cisco Unity server. Subscriber and call management data will be replicated to the secondary Cisco Unity server after you configure failover later in the installation.

22. Define system schedules:
 - a. Identify standard business hours.
 - b. Identify closed and weekend hours.
 - c. Create custom schedules, if necessary.
 - d. Identify holidays.

Refer to the “Schedule Settings” and “Holiday Settings” sections in the “System Settings” chapter.
23. Set up phone, GUI, and TTS languages (including TTY, if applicable). Refer to the “Languages” chapter.
24. Set up third-party fax, if applicable. Refer to the “Integrating a Fax Server with Cisco Unity” chapter.
25. Create a call management plan. Refer to the “Call Management” chapter.
26. Prepare to create regular subscriber accounts. Refer to the “Before Creating Regular Subscriber Accounts” section in the “Creating Subscriber Accounts” chapter.
 - a. Confirm that you have the necessary permissions for creating subscriber accounts and that Cisco Unity is configured properly to work with the message store.
 - b. Confirm that you have the applicable licenses.
 - c. Determine password and account lockout policy for Cisco Unity phone access.
 - d. Determine logon, password, and account lockout policy for Cisco Unity web access.
 - e. Set up enhanced phone security, if applicable.
 - f. Review, change, and create classes of service.
 - g. Create restriction tables, and assign them to the appropriate class(es) of service.
 - h. Create public distribution lists.
 - i. Review, create, and modify subscriber templates. Secure phone passwords, and, as applicable, secure Windows domain account passwords.
 - j. As needed, change the locale ID of the MAPI profile for the Cisco Unity server.
27. Set up the Cisco Unity Hospitality and property management system integration, if applicable. Refer to the “Hospitality and Property Management System Integration” chapter.

28. Test the system configuration:
 - a. Add a single subscriber (refer to the “Creating Subscriber Accounts” chapter).
 - b. Use the phone to log on to Cisco Unity as the test subscriber, record a voice name, and set a phone password. Hang up.
 - c. Call Cisco Unity and log on as the test subscriber again to confirm that the password, greeting, and conversation style specified for the subscriber are working properly. Confirm that the subscriber inherited the correct class of service by testing any applicable features by phone.
 - d. Log on to the Cisco Personal Communications Assistant (PCA) as the test subscriber. If you gave the test subscriber the required class of service rights, test to see if you can browse from the Cisco PCA Welcome page to the Cisco Unity Assistant. If you gave the test subscriber the required class of service rights, test to see if you can browse to the Cisco Unity Inbox.
 - e. Make corrections to the system configuration as necessary.
29. Create subscriber accounts. Refer to the “Creating Subscriber Accounts” chapter.
30. Hide users in the Exchange address book, if applicable. Refer to the “Preventing Subscribers from Appearing in Outlook Address Books” section in the “Creating Subscriber Accounts” chapter.
31. Modify individual subscriber accounts as needed. Refer to the “After Creating Subscriber Accounts” section in the “Creating Subscriber Accounts” chapter.
32. Add individual subscribers to public distribution lists, as needed. (For example, assign subscribers to screen those messages left in Cisco Unity that are not associated with a specific recipient, such as those left to the Unaddressed Messages distribution list or for the Opening Greeting call handler.) Refer to the “Message Handling” section in the “Default Accounts and Message Handling” chapter.
33. Implement, then test the call management plan you created in Task 25.:
 - a. Create call handlers. Refer to the “Call Handler Settings” chapter.
 - b. Specify directory handler settings. Refer to the “Directory Handler Settings” chapter.
 - c. Create interview handlers. Refer to the “Interview Handler Settings” chapter.
 - d. Set up call routing. Refer to the “Call Routing” chapter.
34. Review the substitute objects on the System > Configuration > Settings page of the Cisco Unity Administrator. The objects are Substitute Recipient, Substitute Owner, Substitute After Message Call Handler, and Substitute Exit Call Handler. Cisco Unity uses the objects to substitute references to any subscriber that is deleted by using the Cisco Unity Administrator without first reassigning such references (for example, ownership of a call handler or distribution list). For new installations, the Example Administrator is configured as the Substitute Recipient and Substitute Owner, and the Goodbye call handler is configured as the Substitute After Message Call Handler and Substitute Exit Call Handler. For upgrades, any changes made to the defaults will not be overwritten. However, we recommend that you review these settings now and update them if you wish to use different substitute objects. Refer to Cisco Unity Administrator Help for a description of each object and where it applies.
35. As appropriate, set up subscribers to use their phones to access Cisco Unity, specify their recording and playback device, install Cisco Unity ViewMail for Microsoft Outlook, and set up text-message notifications. Refer to the “Setting Up Cisco Unity Applications on Subscriber Workstations” chapter.

Part 4: Configuring Failover and Setting Up Networking Options (If Applicable)

36. Configure Cisco Unity failover. Refer to the “[Configuring Cisco Unity Failover](#)” chapter of the *Cisco Unity Failover Configuration and Administration Guide, Release 4.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guide_book09186a00801b9241.html.
37. *If the system is using Digital Networking:* Set up Digital Networking. Refer to the “[Digital Networking](#)” chapter of the *Networking in Cisco Unity Guide, Release 4.0(5)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guide_book09186a008044197a.html. (Note that the settings for Digital Networking are replicated to the secondary server.)
38. *If the system is using Internet Subscribers:* Set up Internet subscribers. Refer to the “[SMTP Networking](#)” chapter of the *Networking in Cisco Unity Guide, Release 4.0(5)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guide_book09186a008044197a.html.
39. *If the system is using SMTP Networking:* Set up SMTP Networking. Refer to the “[SMTP Networking](#)” chapter of the *Networking in Cisco Unity Guide, Release 4.0(5)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guide_book09186a008044197a.html. (Note that the settings for SMTP Networking are replicated to the secondary server.)
40. *If the system is using AMIS Networking:* Set up AMIS Networking. Refer to the “[AMIS Networking](#)” chapter of the *Networking in Cisco Unity Guide, Release 4.0(5)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guide_book09186a008044197a.html. (Note that the settings for AMIS Networking are replicated to the secondary server.)
41. *If the system is using VPIM Networking:* Set up VPIM Networking. Refer to the “[VPIM Networking](#)” chapter of the *Networking in Cisco Unity Guide, Release 4.0(5)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guide_book09186a008044197a.html. (Note that the settings for VPIM Networking are replicated to the secondary server.)
42. *If the system is using Bridge Networking:* Install the Cisco Unity Bridge server. Refer to the “[Overview of Mandatory Tasks for Installing the Cisco Unity Bridge](#)” chapter of the applicable *Cisco Unity Bridge Installation Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
43. *If the system is using Bridge Networking:* Set up Cisco Unity and the Bridge for networking. Refer to the “[Setting Up Cisco Unity and the Bridge for Networking](#)” chapter of the applicable *Cisco Unity Bridge Networking Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html. (Note that the settings for the Bridge are replicated to the secondary server.)

Part 5: Customizing the Cisco Unity Conversation

44. When callers access Cisco Unity by phone, they hear a set of prerecorded instructions and options known as the Cisco Unity conversation—or the TUI (telephone user interface). You can customize the conversations that subscribers and unidentified callers hear in several ways.

For example, you may want to change how Cisco Unity handles messages that are interrupted by disconnected calls, specify that Cisco Unity prompts subscribers to record first and then address when they send messages, offer “Easy” Sign-In and system transfers, or specify that Cisco Unity

plays additional caller information when subscribers play messages. You may also want to set up the Cisco Unity Greetings Administrator or the Cisco Unity Broadcast Message Administrator for system administrators to use.

Refer to the “[Cisco Unity Conversation](#)” chapter of the *Cisco Unity System Administration Guide, Release 4.0(5)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_administration_guide_book09186a008043ea39.html for details on these and many other conversation customizations.

Part 6: Backing Up Cisco Unity

45. Back up Cisco Unity. Refer to the “[About Backing Up a Cisco Unity System](#)” chapter of the *Cisco Unity Maintenance Guide, Release 4.0(5)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_maintenance_guide_book09186a008043ea51.html.

Part 7: Training

46. Train subscribers, operators, and support desk personnel to use Cisco Unity. Refer to the “[Preparing Subscribers, Operators, and Support Desk Personnel to Work with Cisco Unity](#)” chapter of the *Cisco Unity System Administration Guide*.



Preparing for the Installation



Note

If you are installing the secondary Cisco Unity server now, skip this chapter.

In this chapter, you do the following tasks in the order listed:

1. Gather the documentation and tools needed for the installation. See the “[Gathering Documentation and Tools](#)” section on page 2-1.
2. Download the software needed for the installation. See the “[Downloading Software for the Installation](#)” section on page 2-2.
3. Determine and record the drive locations for application, log, and database files on the Cisco Unity system. See the “[Determining the Drive Locations for Files on the Cisco Unity Server](#)” section on page 2-4.

When you are finished with this chapter, return to the “[Overview of Mandatory Tasks for Installing Cisco Unity](#)” chapter to continue installing the Cisco Unity system correctly:



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Gathering Documentation and Tools

You need the following items during the installation and configuration of the Cisco Unity system:

- Access to the following Cisco Unity documentation.
 - Release notes for the applicable version of Cisco Unity.
 - Release notes for the applicable Cisco Unity service release, if any.
 - Release notes for the applicable version of Cisco Security Agent for Cisco Unity, if applicable.
 - The correct version of the Cisco Unity installation guide for your configuration. (Refer to the document *Use the Installation Guide That Matches the Cisco Unity 4.0(5) or Later Configuration* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst405/405list.htm.)
 - Specifications for the server on which you are installing Cisco Unity. (Refer to the *Cisco Unity Supported Platforms List*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.)

- The Cisco Unity integration guide(s) for your phone system(s).
- If you are integrating Cisco Unity with Cisco CallManager, release notes for the applicable version of the Cisco Unity-CM TSP.
- The *Cisco Unity System Administration Guide*.
- The *Cisco Unity Failover Configuration and Administration Guide, Release 4.x*.
- If you are setting up Cisco Unity Digital Networking, AMIS, SMTP, or VPIM Networking, or Internet subscribers, the *Networking in Cisco Unity Guide*.
- If you are setting up Bridge Networking, release notes for the applicable version of the Cisco Unity Bridge, the *Cisco Unity Bridge Installation Guide, Release 3.0*, and the *Cisco Unity Bridge Networking Guide, Release 3.0*. Also, release notes for the applicable version of Cisco Security Agent for Cisco Unity Bridge, if applicable.
- If you are setting up AMIS, Bridge, SMTP, or VPIM Networking, release notes for the applicable version of the Cisco Unity Voice Connector for Microsoft Exchange.
- If you anticipate eventually migrating to a Unified Messaging configuration, *White Paper: Installing Cisco Unity Voice Messaging in Anticipation of Migrating to Cisco Unity Unified Messaging (Version 3.1)* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpaper/migvm_um.htm. (Note that although the title refers to Cisco Unity 3.1, the document is also valid for Cisco Unity 4.0.)

Cisco Unity documentation is available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html.

- A blank 3.5-inch 1.44-MB disk for creating an emergency repair disk.
- Two test phones.

Downloading Software for the Installation

This section lists the software needed to install Cisco Unity. Note that if the Cisco Unity DVDs or CDs you have are earlier than the currently shipping version, you must download additional software.

- [Software for All Installations, page 2-3](#)
- [Additional Software for Installations with Cisco Unity DVDs or CDs Earlier Than the Currently Shipping Version, page 2-4](#)

Also note the following considerations:

- The downloads may total 200 MB or more. Use a computer with a high-speed Internet connection, and confirm that the computer has sufficient disk space or has access to a network drive with sufficient disk space.
- The downloads are all self-extracting executable files. When all downloads are complete, extract the updates and burn CDs that contain the extracted files. Then delete the downloaded .exe files to free disk space.

**Caution**

Until you have installed all of the recommended service packs and updates, and, optionally, Cisco Security Agent for Cisco Unity and virus-scanning software, third-party components installed on the Cisco Unity server have significant security vulnerabilities. Do not connect the Cisco Unity server to the network to install software. Instead, burn CDs that contain the downloaded software, and install the software from the CDs.

- The Cisco Unity documentation instructs you when to install the software you download.

Software for All Installations

Download the following software for all installations. Even if you have Cisco Unity DVDs or CDs for the currently shipping version, we recommend that you download the software, some of which may have been released or updated after the discs were produced.

Cisco Unity Service Release

The applicable Cisco Unity service release (a rollup of Cisco Unity engineering specials), if available. Refer to the “Downloading Service Release 1” section of *Release Notes for Cisco Unity <Version> Service Release 1* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html. Note that if there are no release notes available, a service release has not been released.

Microsoft Service Packs

The latest service packs recommended for use with Cisco Unity, if any were qualified after the currently shipping Cisco Unity version was released. Available on the Microsoft website. Also download or print the installation instructions.

To determine the service packs that are recommended, refer to *Recommended Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge* at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/cmptblty/msupdate.htm. (Service packs that were recommended when the currently shipping version was released are available on the Cisco Unity 4.x Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/unity-40>.)

Burn the extracted updates onto a CD labeled “Cisco Unity <Version> Post-Installation.” This is the same disc onto which you would have burned the Cisco Unity service release, if available.

Microsoft Updates

The latest updates recommended for use with Cisco Unity. Available on the Microsoft Updates for Cisco Unity Software Download page at

http://www.cisco.com/cgi-bin/tablebuild.pl/unity_msft_updates. (Updates that were recommended when the currently shipping version of Cisco Unity was released are on the Cisco Unity Post-Install CD, but the download page is updated monthly, so you should check for new updates even if you have the CD.)

**Note**

To access the software download page, you must be logged on to Cisco.com as a registered user.

Cisco Security Agent for Cisco Unity (Optional)

Cisco Security Agent for Cisco Unity is available on the Cisco Unity Crypto Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d>. Refer to *Release Notes for Cisco Security Agent for Cisco Unity* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html for information on supported configurations, and for download and installation instructions.

Because of export controls on strong encryption, the first time you download Cisco Security Agent for Cisco Unity, you need to fill out a brief questionnaire. Follow the on-screen prompts.

Updated PBXLink or PIMG Firmware

If the phone system integration includes PBXLink boxes or PIMG units, updated PBXLink or PIMG firmware. For instructions on downloading updated firmware, refer to the “Setting Up the PBXLink Box” section or the “Setting up the PIMG Units” section in the applicable Cisco Unity integration guide. Integration guides are available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Additional Software for Installations with Cisco Unity DVDs or CDs Earlier Than the Currently Shipping Version

If the Cisco Unity DVDs or CDs you have are earlier than the currently shipping version, you also need to download the following software.

Cisco Unity CDs

CDs for the currently shipping Cisco Unity version. Refer to the “Downloading Software for Cisco Unity <Version>” section of the applicable *Release Notes for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Cisco Unity Service Pack CDs

The Cisco Unity Service Pack CD that contains the service pack for the version of Exchange you are using. Refer to the “Downloading Software for Cisco Unity <Version>” section of the applicable *Release Notes for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Determining the Drive Locations for Files on the Cisco Unity Server

You plan drive locations for application, log, and database files on the Cisco Unity server:

- To maximize performance, data integrity, and reliability for Cisco Unity, Microsoft Exchange, and SQL Server transaction logs.
- To maximize performance, data storage, and access capacity for Cisco Unity data.

The way in which logical drives on the Cisco Unity server are set up and the drive locations for application, log, and database files depend on the platform overlay of the Cisco Unity server and the RAID volume configuration used.

**Note**

The file locations must be the same on the primary and secondary Cisco Unity servers.

Using one of the following sections, make note of the applicable drive locations for files on the Cisco Unity server that you are installing:

- [Drive Locations for Files on a Platform Overlay 1 Server, page 2-5](#)
- [Drive Locations for Files on a Platform Overlay 2 Server, page 2-5](#)
- [Drive Locations for Files on a Platform Overlay 3 Server, page 2-6](#)

For information on the platform overlay, RAID configuration, maximum number of Cisco Unity subscribers, and other specifications for the server on which you are installing Cisco Unity, refer to the *Cisco Unity Supported Platforms List*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.

The Cisco Unity installation guide alerts you when to refer to the file locations later in the installation process.

Drive Locations for Files on a Platform Overlay 1 Server

[Table 2-1](#) lists the drive locations for currently shipping Cisco Unity Platform Overlay 1 servers.

**Note**

Except for the system drive, drive C, different drive letters may be used to label the drives.

Table 2-1 *Drive Locations for Files on a Platform Overlay 1 Server*

Logical Drive	Files
C	<ul style="list-style-type: none"> • Operating system • Pagefile
D	<ul style="list-style-type: none"> • SQL Server 2000 databases • SQL Server 2000 transaction logs • Unity Message Repository (UMR) • Program files, including Cisco Unity and SQL Server 2000 • Cisco Unity trace logs

Drive Locations for Files on a Platform Overlay 2 Server

[Table 2-2](#) lists the drive locations for currently shipping Cisco Unity Platform Overlay 2 servers.

**Note**

Except for the system drive, drive C, different drive letters may be used to label the drives.

Table 2-2 Drive Locations for Files on a Platform Overlay 2 Server

Disk Array	Logical Drive	Files
First	C	<ul style="list-style-type: none"> Operating system Pagefile
First	D	<ul style="list-style-type: none"> SQL Server 2000 transaction logs Program files, including Cisco Unity and SQL Server 2000 Cisco Unity trace logs
Second	E	<ul style="list-style-type: none"> SQL Server 2000 databases Unity Message Repository (UMR)

Drive Locations for Files on a Platform Overlay 3 Server

Table 2-3 lists the drive locations for currently shipping Cisco Unity Platform Overlay 3 servers.


Note

Except for the system drive, drive C, different drive letters may be used to label the drives.

Table 2-3 Drive Locations for Files on a Platform Overlay 3 Server

Disk Array	Logical Drive	Files
First	C	<ul style="list-style-type: none"> Operating system Pagefile
First	D	<ul style="list-style-type: none"> Program files, including Cisco Unity and SQL Server 2000 Cisco Unity trace logs SQL Server transaction logs
Second	E	<ul style="list-style-type: none"> SQL Server 2000 databases Unity Message Repository (UMR)



Setting Up the Hardware

In this chapter, you do the following tasks in the order listed:

1. *If the Cisco Unity system is using voice cards to integrate with a circuit-switched phone system:* Install voice cards. See the [“Installing Voice Cards”](#) section on page 3-1.
2. Set up the Cisco Unity server. See the [“Attaching Peripheral Devices and Making Connections from the Phone System”](#) section on page 3-5.

When you are finished with this chapter, return to the [“Overview of Mandatory Tasks for Installing Cisco Unity”](#) chapter to continue installing the Cisco Unity system correctly.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Installing Voice Cards



Note

If the system is not using voice cards to integrate with a circuit-switched phone system, skip this section.

All voice cards must be installed in the same server or in the same expansion chassis. If all voice cards do not fit in the Cisco Unity server, then you must install all of them in an expansion chassis.

All Cisco Unity-compatible voice cards are 33-MHz PCI cards. Universal PCI (uPCI) cards work in either 5-Vdc or 3.3-Vdc PCI and PCI-X slots, while non-universal PCI cards work only in 33-MHz (5-Vdc) slots.

If you are installing a uPCI voice card, you can generally place the card in any physically compatible slot in the server or expansion chassis. However, if the slot you choose is a 3.3-Vdc PCI or PCI-X slot (designed to be 66 MHz or faster), that slot and the slot adjacent to it on the same logical PCI bus segment will slow down to 33 MHz to accommodate the 33-MHz card. (For example, if a 33-MHz voice card is placed in a PCI-X slot next to a 133-MHz RAID controller and they share the same logical segment, the RAID controller speed is reduced to 33 MHz.)

Refer to the manufacturer documentation for detailed PCI bus topology information before deciding final slot placement of 3.3-Vdc or 5-Vdc, 33-MHz voice cards.

Note that if you view a voice card by using Windows Device Manager, the card may be displayed as an unknown PCI device, with a warning stating that the drivers for the device are not installed. A Found New Hardware wizard may also appear for each card during installation or when the Cisco Unity server is restarted. These conditions are both expected behavior, and do not indicate an error or a condition

requiring action. You can disable the Found New Hardware wizard to prevent it from appearing when the Cisco Unity server is restarted. The Cisco Unity installation guide alerts you when to do the procedure later in the installation process (“[Disabling the Found New Hardware Wizard for the Voice Cards](#)” section on page 5-10).



Warning

This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.

Statement 1017



Warning

Read the installation instructions before connecting the system to the power source. Statement 1004



Warning

Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.

Statement 1



Warning

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024



Warning

There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. Statement 1015



Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006



Warning

Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages. Statement 2



Warning

Do not work on the system or connect or disconnect cables during periods of lightning activity.

Statement 1001



Warning

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord. Statement 1023

**Warning**

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
Statement 1030

**Warning**

This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel. Statement 88

**Warning**

The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards. Statement 117

**Warning**

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.
Statement 1029

To Install Voice Cards in the Cisco Unity Server or in an Expansion Chassis

- Step 1** If the server is on, shut it down.
- Step 2** Unplug the power cord.
- Step 3** Attach an antistatic wrist strap, and ground yourself to the server.

**Warning**

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.
Statement 94

- Step 4** Set the switches and jumpers on each card. See the “Hardware Settings” section for your cards in the “Voice Cards and PIMG Units” appendix.
- Some cards include hardware settings that indicate which card is first, which is second, and so on. If you are installing more than one card of the same model, keep the cards in order so you can install them in the correct order in [Step 6](#).
- If you are installing Intel Dialogic D/120JCT-Euro or D/240PCI-T1 cards, do not do the procedure in the “Software Settings” section for your cards in the “Voice Cards and PIMG Units” appendix at this time. The Cisco Unity installation guide alerts you when to do the procedure later in the installation process.
- Step 5** If you are not using a PCI expansion chassis, skip to [Step 6](#).
- If you are using a PCI expansion chassis, install the host card in an applicable slot, depending on the platform. Use the required host-card slot with the following platforms:

Platform	Required Host-Card Slot
Cisco MCS-7835-I1-ECS1	Slot 3 or 4
Cisco MCS-7845-I1-ECS1	Slot 3 or 4

Platform	Required Host-Card Slot
Cisco MCS-7845-I1-ECS2	Slot 3 or 4
Dell PowerEdge 4400	Slot 1
Hewlett-Packard DL580G1	Slot 6
Hewlett-Packard DL580G2	Slot 4 to 6
Hewlett-Packard ML570G1	Slot 6
Hewlett-Packard ML570G2	Slot 4 to 6
IBM x Series 232	Slot 4
IBM x Series 342	Slot 4
IBM x Series 345	Slot 3 or 5
IBM x Series 346	Slot 3 or 4



Note The slot assignments shown in the table do not apply to voice cards.

For supported platforms that are not listed above, the host card can be installed in any applicable slot. (For the platforms that support using an expansion chassis, refer to the *Cisco Unity Supported Platforms List*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.)

Note that if the slot location of a customer-provided server management card (such as Hewlett-Packard Remote Insight Lights-Out Edition) conflicts with a required host card slot, the host card takes precedence.

Step 6 Insert each voice card firmly into its slot in the server or in the expansion chassis, and fasten each card to the back plate with a screw. Note the following considerations, as applicable:

- If you are installing more than one voice card of the same model, and if the cards include a hardware setting that indicates which card is first, second, and so on, install the cards in the order specified by the hardware settings.
- If you are installing voice cards of different models in the same server, install cards of the same model adjacent to one another.
- Choose a physically compatible slot in an appropriate bus segment. Refer to the manufacturer documentation for detailed PCI bus topology information.



Caution Placing a 33-MHz Intel Dialogic voice card in a physical interface slot in the same logical segment as a 66-MHz PCI or 100-to-133-MHz PCI-X interface card will slow both slots in the logical segment to 33 MHz, degrading performance of the whole platform.

Step 7 If you are installing multiple voice cards that have H.100 bus connectors, cable the cards together. On each card, connect the cable so the red stripe on the cable corresponds with pin 1 on the card connector. Confirm that the connectors are firmly seated.



Caution If you do not cable cards together as required, the voice card software will not start, and Cisco Unity will not answer calls.

If the cable has more connectors than the server has voice cards, use the first and last connectors, and leave unused connectors in the middle of the cable. If the end of a cable is allowed to dangle loose, it can act as a radio antenna and pick up noise from the bus.

If you are cabling three or more cards together, connect the first connector on the cable to the first card, the second connector to the second card, and so on.

Attaching Peripheral Devices and Making Connections from the Phone System

We recommend that you connect the Cisco Unity server to a dedicated uninterruptible power supply.

A Cisco Unity server purchased from Cisco is configured for a specific hardware setup. Do not add or change any hardware on the server, except to add voice cards, memory, a tape drive, an external modem, or a rail kit.

To Attach Peripheral Devices and Make Connections from the Phone System

- Step 1** Place the server in a dry, cool area that is free of dust. Note the following considerations, as applicable:
- If the Cisco Unity server will be connected to the network, place it near a network connection.
 - If the Cisco Unity system is using voice cards to integrate with a circuit-switched phone system, place the server near the phone system.
 - If the Cisco Unity system is using PIMG units to integrate with a circuit-switched phone system, place the PIMG units near the phone system and near a network connection.



Caution Do not attach the network cable to the server until you have installed the Microsoft service packs and updates recommended for use with Cisco Unity. The Cisco Unity installation guide alerts you when to install the service packs and updates, and when to connect to the network later in the installation process.

- Step 2** Attach any supported peripheral devices to the server. Follow the manufacturer installation and test instructions.

- Step 3** Make the connections from the phone system, depending on whether the system is using voice cards or PIMG units for the integration:

Voice cards with a circuit-switched phone system	Connect the phone system to the Cisco Unity server as described in the applicable Cisco Unity integration guide for the phone system. For pinout information, see the applicable voice card section in the “Voice Cards and PIMG Units” appendix.
PIMG units with a circuit-switched phone system	Connect the phone system to the PIMG units as described in the applicable Cisco Unity integration guide for the phone system. For pinout information, see the “Intel NetStructure PBX-IP Media Gateway (PIMG)” section on page A-11.

Cisco Unity integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

- Step 4** If you are installing the Cisco Unity system outside the United States and the server contains voice cards that came with a ferrite clamp, attach the clamp around the analog phone lines as close to the server as possible.



Installing the Operating System

In this chapter, you do the following tasks in the order listed:

1. *If the system is using RAID:* Configure the RAID arrays. See the [“Configuring the RAID Arrays” section on page 4-1](#).
2. Install Windows Server 2003 or Windows 2000 Server. See the [“Installing Windows Server 2003 or Windows 2000 Server” section on page 4-3](#).
3. *If the system is running Windows Server 2003:* Enable Windows Terminal Services. See the [“Enabling Windows Terminal Services \(Windows Server 2003 Only\)” section on page 4-9](#).
4. *If the Cisco Unity server was not purchased from Cisco or if the system is running Windows Server 2003:* Set up the logical drives according to the storage configuration requirements for the platform. See the [“Setting Up the Logical Drives” section on page 4-9](#).

(Note that a Cisco Unity server purchased from Cisco to run Windows 2000 Server was shipped with Platform Configuration discs that automatically set up the logical drives when the discs were used to install Windows 2000 in Task 2.)

When you are finished with this chapter, return to the [“Overview of Mandatory Tasks for Installing Cisco Unity”](#) chapter to continue installing the Cisco Unity system correctly.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Configuring the RAID Arrays



Note

If the system is not using RAID, skip this section.

Do this section only if the system is using hardware-based RAID. (Software-based RAID is not supported.)

To configure the arrays, you group the physical disks into logical disks and assign a RAID type to each logical disk. The procedure you use to configure the arrays depends on whether the Cisco Unity server was purchased from Cisco:

Server purchased from Cisco	<p>Use the Cisco-provided array-configuration utility. See the “Using the Cisco-Provided Array-Configuration Utility” section on page 4-2.</p> <p>Note We recommend that you use the Cisco-provided array-configuration utility that appears on the Cisco Unity Platform and RAID Configuration Disc even if you install the operating system by using the manufacturer’s guided system-setup utility and a retail Windows disc. The array-configuration utility automatically configures the arrays as recommended for each server and can save a substantial amount of time over manually configuring the arrays by using the array-configuration utility available on the manufacturer disc.</p>
Server not purchased from Cisco	<p>Use the array-configuration utility available on the manufacturer disc that is shipped with the Cisco Unity server. See the “Using the Manufacturer-Provided Array-Configuration Utility” section on page 4-3.</p>

Using the Cisco-Provided Array-Configuration Utility

A Cisco Unity server purchased from Cisco ships with Platform Configuration discs that contain a utility for automatically configuring the arrays. Do one of the following two procedures, depending on the platform: Hewlett-Packard or IBM.

Hewlett-Packard: To Configure the RAID Arrays by Using the Cisco-Provided Utility

-
- Step 1** Start the Cisco Unity server, and insert Cisco Unity Platform and RAID Configuration Disc (HP) CD 1 in the CD-ROM drive.
- Step 2** When the main menu appears, press <F1>.
- Step 3** Follow the on-screen prompts. When the utility has completed, the main menu reappears.



Caution Do not press any keys while the BIOS screen is displayed. If you interrupt the utility, you will have to start over.

IBM: To Configure the RAID Arrays by Using the Cisco-Provided Utility

-
- Step 1** Start the Cisco Unity server, and insert the Cisco Unity RAID Configuration Disc (IBM) in the CD-ROM drive.
- Step 2** Select the server type. The options may combine the following information:
- Server model.
 - Number of physical disks installed in the server.
 - Size, in gigabytes, of the largest physical disks.

- Step 3** Press **Enter**.
- Step 4** Follow the on-screen prompts.

Using the Manufacturer-Provided Array-Configuration Utility

The server manufacturer provides a disc that contains utilities for several setup tasks, including configuring RAID arrays. Use the disc to configure the arrays when the Cisco Unity server was not purchased from Cisco.

The following discs are provided by server manufacturers:

Hewlett-Packard	Hewlett-Packard SmartStart
IBM	IBM ServerGuide

The following procedure contains only general steps. For detailed instructions on using a specific array-configuration utility, refer to the manufacturer documentation.

To Configure the RAID Arrays by Using the Manufacturer-Provided Utility

- Step 1** Start the Cisco Unity server, and insert the manufacturer disc in the CD-ROM drive.
- Step 2** On the main menu, select the array-configuration utility.
- Step 3** For each logical disk needed, group physical disks of the same make and model, and assign a RAID type. For information on the recommended RAID configuration for the server, refer to the *Cisco Unity Supported Platforms List*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.
- Step 4** Follow the manufacturer instructions to complete the configuration.

Installing Windows Server 2003 or Windows 2000 Server

If you are installing Windows Server 2003, you must use the manufacturer's guided system-setup utility and a retail Windows Server 2003 disc in the desired language. Cisco Unity Platform Configuration discs with Windows Server 2003 are not available, and Windows Server 2003 is not available when you purchase a Cisco Unity server from Cisco. See the "Windows Server 2003: Using the Manufacturer's Guided System-Setup Utility and a Retail Windows Server 2003 Disc" section on page 4-4.



Caution

If you install Windows Server 2003, do not install Universal Description, Discovery, and Integration (UDDI) Services, or the Cisco Unity System Preparation Assistant will fail later in the installation process.

If you are installing Windows 2000 Server, the compact discs you use depend on whether the Cisco Unity server was purchased from Cisco and which language version of Windows 2000 Server you want to install:

Server purchased from Cisco, and installing the English-language version of Windows 2000 Server	Use the Platform Configuration discs that are shipped with the Cisco Unity server. See the “Windows 2000 Server: Using the Cisco Unity Platform Configuration Discs” section on page 4-5.
Server not purchased from Cisco, or installing a localized version of Windows 2000 Server	Use the manufacturer’s guided system-setup utility and a retail Windows 2000 Server disc in the desired language. See the “Windows 2000 Server: Using the Manufacturer’s Guided System-Setup Utility and a Retail Windows 2000 Server Disc” section on page 4-7.

Windows Server 2003: Using the Manufacturer’s Guided System-Setup Utility and a Retail Windows Server 2003 Disc

The server manufacturer provides a disc that contains utilities for several setup tasks, including guiding the installation of Windows 2003 Server from a retail disc. Always use the manufacturer’s guided system-setup utility to install Windows Server 2003. This ensures that the operating system and the drivers are installed and configured correctly.



Note

Cisco Unity Platform Configuration discs are not available for Windows Server 2003.

The following discs are provided by server manufacturers:

Hewlett-Packard	Hewlett-Packard SmartStart
IBM	IBM ServerGuide



Caution

Do not attach the network cable to the server until you have installed the Microsoft service packs and updates recommended for use with Cisco Unity. The Cisco Unity installation guide alerts you when to install the service packs and updates, and when to connect to the network later in the installation process.

To Install Windows Server 2003 by Using the Manufacturer’s Guided System-Setup Utility and a Retail Windows 2003 Disc

Step 1 Start the Cisco Unity server, and insert the manufacturer disc in the CD-ROM drive.

Step 2 Follow the on-screen prompts to install Windows Server 2003 from a retail disc.

You may be prompted to configure the RAID arrays. Note the following considerations:

- If the arrays have already been configured, do not change the configuration.
- If the arrays have not been configured, follow the prompts to configure them. Refer to the manufacturer documentation.

Step 3 When applicable, make the following choices:

- Specify a partition size of **8 GB** for the operating system.
- If you are installing Windows Server 2003 on the same partition where an operating system is already installed, select and delete that partition.
- Format the operating system partition by using the **NTFS** file system.
- For regional settings, select a locale in the Your Locale (Location) list. The locale you select must match one of the languages that you will install for Cisco Unity. Note that the Cisco Unity installation always installs English (United States).

For a list of supported languages, refer to *Cisco Unity 4.0 System Requirements and Supported Hardware and Software* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm.

**Caution**

If the locale you specify when you install Windows Server 2003 does not match any of the installed Cisco Unity languages, Cisco Unity will log errors in the event log and may stop taking calls. The locale you select here must match the Cisco Unity language exactly. For example, if you choose English (United Kingdom) for locale, you must also choose English (United Kingdom) as one of the Cisco Unity languages. Installing the Cisco Unity language English (Australia) will not work.

- Specify **Per Seat** for the licensing mode.
- When you enter a name (netBIOS name) for the Cisco Unity server:
 - Use a name that is 15 characters or fewer in length.
 - Use only alphabetical characters A to Z and a to z, numerical characters 0 to 9, and hyphens (-).

**Caution**

Using other characters in the server name is not supported by DNS.

- Do not join a domain. Instead, specify a workgroup. The Cisco Unity installation guide alerts you when to connect to the network and when to join a domain later in the installation process.

Windows 2000 Server: Using the Cisco Unity Platform Configuration Discs

A Cisco Unity server purchased from Cisco ships with Platform Configuration discs that contain a utility to install Windows 2000 Server by restoring an image that is customized for the platform. The image includes the required Windows 2000 Server components, subcomponents, and service packs (for example, Internet Information Services, Terminal Services, and the required Windows 2000 Server service pack).

Installing Windows 2000 Server by using the Cisco Unity Platform Configuration discs reduces the Cisco Unity system installation time and ensures that the required operating system and components, drivers, and service packs are installed and configured correctly. In addition, the logical drives are automatically set up.

**Caution**

Do not attach the network cable to the server until you have installed the Microsoft service packs and updates recommended for use with Cisco Unity. The Cisco Unity installation guide alerts you when to install the service packs and updates, and when to connect to the network later in the installation process.

Do one of the following two procedures, depending on the platform: Hewlett-Packard or IBM.

Hewlett-Packard: To Install Windows 2000 Server by Using the Cisco Unity Platform Configuration Discs

-
- Step 1** Start the Cisco Unity server, and insert Cisco Unity Platform and RAID Configuration Disc (HP) CD 1 in the CD-ROM drive.
 - Step 2** When the main menu appears, press <F2>.
 - Step 3** Follow the on-screen prompts until you are prompted to remove the disc from the drive.
 - Step 4** Remove CD 1, and insert Cisco Unity Platform and RAID Configuration Disc (HP) CD 2 in the CD-ROM drive.
 - Step 5** Follow the on-screen prompts until you are prompted to select a licensing mode.
 - Step 6** Click **Per Seat**, and click **Next**.
 - Step 7** Enter a name for the Cisco Unity server (netBIOS name). Use only alphabetical characters A to Z and a to z, numerical characters 0 to 9, and hyphens (-).



Caution Using other characters in the server name is not supported by DNS.

The server name must be 15 characters or fewer in length.

- Step 8** Specify and confirm a password, then click **Next**.
- Step 9** Follow the on-screen prompts until the Network Settings dialog box appears.
- Step 10** Click **Typical Settings**, and click **Next**.
- Step 11** In the Workgroup or Computer Domain dialog box, click **No, This Computer Is Not on a Network, or Is on a Network Without a Domain**.
If the Workgroup or Computer Domain dialog box is empty, enter a workgroup name. The name you enter now is not important. You will join a domain or make the Cisco Unity server a domain controller in a later procedure, so the Cisco Unity server will no longer be in a workgroup.
- Step 12** Click **Next**.
- Step 13** Follow the on-screen prompts to complete the installation.
- Step 14** When the Windows 2000 Configure Your Server dialog box appears, click **I Will Configure This Server Later**, and click **Next**.
- Step 15** Uncheck the **Show This Screen at Startup** check box, and close the window.

IBM: To Install Windows 2000 Server by Using the Cisco Unity Platform Configuration Discs

-
- Step 1** Start the Cisco Unity server, and insert Cisco Unity Platform Configuration Disc (IBM) CD 1 in the CD-ROM drive.
 - Step 2** When the main menu appears, press **Enter** to start the installation program.
 - Step 3** Follow the on-screen prompts until you are prompted to select a licensing mode.
 - Step 4** Click **Per Seat**, and click **Next**.

- Step 5** Enter a name for the Cisco Unity server (netBIOS name). Use only alphabetical characters A to Z and a to z, numerical characters 0 to 9, and hyphens (-).



Caution Using other characters in the server name is not supported by DNS.

The server name must be 15 characters or fewer in length.

- Step 6** Specify and confirm a password, then click **Next**.
- Step 7** Follow the on-screen prompts until the Network Settings dialog box appears.
- Step 8** Click **Typical Settings**, and click **Next**.
- Step 9** In the Workgroup or Computer Domain dialog box, click **No, This Computer Is Not on a Network, or Is on a Network Without a Domain**.
- If the Workgroup or Computer Domain box is empty, enter a workgroup name. The name you enter now is not important. You will join a domain or make the Cisco Unity server a domain controller in a later procedure, so the Cisco Unity server will no longer be in a workgroup.
- Step 10** Click **Next**.
- Step 11** Follow the on-screen prompts to complete the installation.
- Step 12** When the Windows 2000 Configure Your Server dialog box appears, click **I Will Configure This Server Later**, and click **Next**.
- Step 13** Uncheck the **Show This Screen at Startup** check box, and close the window.

Windows 2000 Server: Using the Manufacturer's Guided System-Setup Utility and a Retail Windows 2000 Server Disc

The server manufacturer provides a disc that contains utilities for several setup tasks, including guiding the installation of Windows 2000 Server from a retail disc. Use the manufacturer disc when the Cisco Unity server was not purchased from Cisco.

The following discs are provided by server manufacturers:

Hewlett-Packard	Hewlett-Packard SmartStart
IBM	IBM ServerGuide

Installing Windows 2000 Server by using the manufacturer's guided system-setup utility ensures that the operating system and the drivers are installed and configured correctly.



Caution

Do not attach the network cable to the server until you have installed the Microsoft service packs and updates recommended for use with Cisco Unity. The Cisco Unity installation guide alerts you when to install the service packs and updates, and when to connect to the network later in the installation process.

To Install Windows 2000 Server by Using the Manufacturer's Guided System-Setup Utility and a Retail Windows 2000 Disc

Step 1 Start the Cisco Unity server, and insert the manufacturer disc in the CD-ROM drive.

Step 2 Follow the on-screen prompts to install Windows 2000 Server from a retail disc.

You may be prompted to configure the RAID arrays. Note the following considerations:

- If the arrays have already been configured, do not change the configuration.
- If the arrays have not been configured, follow the prompts to configure them. Refer to the manufacturer documentation.

Step 3 When applicable, make the following choices:

- Specify a partition size of **8 GB** for the operating system.
- If you are installing Windows 2000 Server on the same partition where an operating system is already installed, select and delete that partition.
- Format the operating system partition by using the **NTFS** file system.
- For regional settings, select a locale in the Your Locale (Location) list. The locale you select must match one of the languages that you will install for Cisco Unity. Note that the Cisco Unity installation always installs English (United States).

For a list of supported languages, refer to *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm.



Caution

If the locale you specify when you install Windows 2000 Server does not match any of the installed Cisco Unity languages, Cisco Unity will log errors in the event log and may stop taking calls. The locale you select here must match the Cisco Unity language exactly. For example, if you choose English (United Kingdom) for locale, you must also choose English (United Kingdom) as one of the Cisco Unity languages. Installing the Cisco Unity language English (Australia) will not work.

- Specify **Per Seat** for the licensing mode.
- When you enter a name for the Cisco Unity server (netBIOS name), use only alphabetical characters A to Z and a to z, numerical characters 0 to 9, and hyphens (-).



Caution

Using other characters in the server name is not supported by DNS.

The server name must be 15 characters or fewer in length.

- Do not join a domain. Instead, specify a workgroup. The Cisco Unity installation guide alerts you when to connect to the network and when to join a domain later in the installation process.

- If you are prompted to specify Windows 2000 Server components to install, select the following required components:
 - Internet Information Services
 - Message Queuing Services
 - Terminal Services



Note If you do not install all the required Windows 2000 Server components, subcomponents, and service packs while installing the operating system, the Cisco Unity installation guide alerts you when and how to install them later.

- Step 4** When the Windows 2000 Configure Your Server dialog box appears, click **I Will Configure This Server Later**.
- Step 5** Uncheck the **Show This Screen at Startup** check box, and close the window.

Enabling Windows Terminal Services (Windows Server 2003 Only)



Note If the system is running Windows 2000 Server, skip this section.

Windows Terminal Services is installed when you install Windows Server 2003, but it is not enabled. You enable Terminal Services so Cisco TAC can access the Cisco Unity server if necessary.

To Enable Windows Terminal Services

- Step 1** On the Windows Start menu, click **Control Panel > System**.
- Step 2** In the System Properties dialog, click the **Remote** tab.
- Step 3** Check the **Allow Users to Connect Remotely to This Computer** check box.
- Step 4** Click **OK** to dismiss the Remote Sessions message box.
- Step 5** Click **OK** to save your changes and close the System Properties dialog box.

Setting Up the Logical Drives



Note If the Cisco Unity server was purchased from Cisco and is running Windows 2000 Server, skip this section. When you installed Windows 2000 Server with the Cisco Unity Platform Configuration discs shipped with the server, the logical drives were set up automatically.

To set up a logical drive, you create an extended partition on a logical disk, then create the logical drive in the partition. Do the following procedure to set up all the drives that you identified in the [“Determining the Drive Locations for Files on the Cisco Unity Server”](#) section on page 2-4.

To Set Up the Logical Drives

- Step 1** Log on to Windows as a member of the Administrators group.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Computer Management**.
- Step 3** In the console tree under Storage, click **Disk Management**.
- Step 4** Right-click the first available unallocated region of the first available logical disk, and click **Create Partition**.

Typically, you will need to create one more logical drive than the number of logical disks available. After you install the operating system, the first 8 GB of the first logical disk is used for the system partition, and is given the drive letter C. You create the first extended partition by using the remaining space on the first logical disk. When you create subsequent partitions, you use the entire logical disk. If you need the same number of logical drives as the number of logical disks available, use an entire logical disk for each partition you create.

- Step 5** On the Create Partition Wizard welcome screen, click **Next**.
 - Step 6** Click **Extended Partition**, and click **Next**. (Do not click Primary Partition.)
 - Step 7** Specify to use the remaining disk space, and click **Next**.
 - Step 8** Verify the settings, and click **Finish**.
 - Step 9** In the Disk Management utility, right-click the new partition, and click **Create Logical Drive**.
 - Step 10** On the Create Partition Wizard welcome screen, click **Next**.
 - Step 11** Click **Logical Drive**, and click **Next**.
 - Step 12** Specify to use the maximum disk space, and click **Next**.
 - Step 13** Assign a drive letter, and click **Next**.
 - Step 14** Specify to use the NTFS file system format, and click **Next**.
 - Step 15** Verify the settings, and click **Finish**.
 - Step 16** Repeat [Step 4](#) through [Step 15](#) for each logical drive that you have to create.
-



Customizing the Cisco Unity Platform

In this chapter, you do the following tasks in the order listed:

1. *If the Cisco Unity server contains a dual NIC:* Configure the dual NIC or verify the configuration. See the [“Configuring a Dual NIC in the Cisco Unity Server”](#) section on page 5-2.
2. Complete registration information on Cisco.com to obtain the applicable license files. See the [“Obtaining Cisco Unity License Files”](#) section on page 5-4.
3. Use the Cisco Unity System Preparation Assistant to install required Windows components, the browser and database, and required service packs. See the [“Running the Cisco Unity System Preparation Assistant”](#) section on page 5-6.
4. Change folder settings in Windows Explorer so that all files and folders are visible during Cisco Unity troubleshooting, if applicable. See the [“Changing Folder Settings in Windows Explorer”](#) section on page 5-8.
5. Install the latest Microsoft service packs and updates for Windows, Internet Explorer, and SQL Server 2000 that are recommended for use with Cisco Unity. See the [“Installing the Latest Microsoft Service Packs and Updates for Windows, Internet Explorer, and SQL Server 2000”](#) section on page 5-9.
6. *If the Cisco Unity server contains voice cards:* Disable the Found New Hardware wizard, if applicable. See the [“Disabling the Found New Hardware Wizard for the Voice Cards”](#) section on page 5-10.
7. *Optional:* Install virus-scanning software. See the [“Installing Virus-Scanning Software \(Optional\)”](#) section on page 5-10.
8. *Optional:* Install and configure Cisco Security Agent for Cisco Unity. See the [“Installing and Configuring Cisco Security Agent for Cisco Unity \(Optional\)”](#) section on page 5-11.
9. Connect the Cisco Unity server to the network. See the [“Connecting the Cisco Unity Server to the Network”](#) section on page 5-11.
10. Configure TCP/IP properties See the [“Configuring TCP/IP Properties”](#) section on page 5-11.
11. Confirm that the server has a valid IP address and is connected to the network. See the [“Verifying the IP Address and the Network Connection”](#) section on page 5-12.
12. *If virus-scanning software or Cisco Security Agent for Cisco Unity is installed on the Cisco Unity server:* Disable virus-scanning services and Cisco Security Agent for Cisco Unity. See the [“Disabling Virus-Scanning and Cisco Security Agent Services”](#) section on page 5-12.
13. Add the Cisco Unity server to an existing domain. See the [“Adding the Cisco Unity Server to an Existing Domain”](#) section on page 5-13.

14. Reset the account that SQL Server services log on as. See the [“Resetting the Account That SQL Server Services Log On As”](#) section on page 5-14.

When you are finished with this chapter, return to the [“Overview of Mandatory Tasks for Installing Cisco Unity”](#) chapter to continue installing the Cisco Unity system.

**Note**

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Configuring a Dual NIC in the Cisco Unity Server

**Note**

If the Cisco Unity server does not contain a dual NIC, skip this section.

We recommend that a dual NIC be configured in adapter fault tolerant mode (AFT) or network fault tolerant (NFT) mode. One NIC is designated as the primary and the other NIC as the secondary for active-passive fault tolerance. In this configuration, the primary (active) NIC handles 100 percent of the traffic. Only in the event that the primary NIC becomes unavailable does the secondary NIC then become active and handle 100 percent of the traffic.

Alternatively, if you do not want to configure AFT or NFT, or do not have a second LAN port available, the following configurations are supported, though not recommended:

- Disable TCP/IP for the second NIC, which allows you to re-enable the second NIC remotely if the first NIC fails. (Use the Network and Dial-up Connections Control Panel to disable TCP/IP for the second NIC.)
- Disable the second NIC in the BIOS. (On some Cisco Unity servers, the second NIC is disabled in the BIOS by default.)

**Caution**

Note that not plugging a network cable into the second NIC is not sufficient. You must either disable TCP/IP for the second NIC or disable the second NIC in the BIOS, or Cisco Unity may not work properly.

If you installed Windows 2000 Server by using the Cisco Unity Platform Configuration discs, skip to the [“Configuring a Dual NIC”](#) section on page 5-4. (The NIC-configuration utility was installed automatically.)

If you installed Windows Server 2003 or if you installed Windows 2000 Server by using a retail Windows disc, you need to install the NIC-configuration utility before you can configure the dual NIC. Do the applicable procedures in the following two sections.

Installing the NIC-Configuration Utility

**Note**

If you installed Windows 2000 Server by using the Cisco Unity Platform Configuration discs, skip this section.

Do the applicable procedure in this section, depending on whether the Cisco Unity server was manufactured by Hewlett-Packard or IBM and, for IBM, depending on whether you have an Intel or a Broadcom installation disc (the disc corresponds with the brand of NIC installed in the server):

- [To Install the Hewlett-Packard NIC-Configuration Utility, page 5-3](#)
- [To Install the IBM NIC-Configuration Utility by Using a Broadcom Disc, page 5-3](#)
- [To Install the IBM NIC-Configuration Utility by Using an Intel Disc, page 5-3](#)

(Cisco-branded servers that have a model number ending in “H” were manufactured by Hewlett-Packard. Cisco-branded servers that have a model number ending in “I” were manufactured by IBM.)

**Note**

The following procedures are intended for the software shipped with the currently shipping Cisco Unity servers. Procedures for older servers may differ.

To Install the Hewlett-Packard NIC-Configuration Utility

- Step 1** Insert the Hewlett-Packard SmartStart disc in the CD-ROM drive.
 - Step 2** Browse to the directory **Compaq\Csp\Nt**, and double-click **Setup.exe**.
 - Step 3** In the right pane of the HP Remote Deployment utility, select and delete all items except HP ProLiant Network Configuration Utility <version> for Windows <2003/2000>.
 - Step 4** Click **Install**.
 - Step 5** Follow the on-screen prompts to complete the installation.
-

To Install the IBM NIC-Configuration Utility by Using a Broadcom Disc

- Step 1** Insert the Broadcom NetXtreme Gigabit Ethernet Software disc in the CD-ROM drive.
If the installation program does not appear automatically, browse to the root of the CD, and double-click **Launch.exe**.
 - Step 2** In the installation program, click **Management Programs**.
 - Step 3** Follow the on-screen prompts until you are prompted to select the applications to install.
 - Step 4** Check the **Control Suite** and **BASP** check boxes.
 - Step 5** Follow the on-screen prompts to complete the installation.
-

To Install the IBM NIC-Configuration Utility by Using an Intel Disc

- Step 1** Insert the Intel Ethernet Software disc in the CD-ROM drive.
If the installation program does not appear automatically, browse to the root of the CD, and double-click **Autorun.exe**.
 - Step 2** Follow the on-screen prompts to complete the installation of the Intel NIC-configuration utility.
-

Configuring a Dual NIC

To Configure a Dual NIC in the Cisco Unity Server

- Step 1** Start the NIC-configuration utility:
- On the Windows Start menu, click **Settings > Control Panel**.
 - Select the applicable option, depending on the server model and NIC brand:

Hewlett-Packard or Cisco MCS server with model number ending in "H"	Click HP Network .
IBM or Cisco MCS server with model number ending in "I"	<ul style="list-style-type: none"> For a Broadcom dual NIC, click Broadcom Control Suite 2. For an Intel dual NIC, click Intel(R) PROSet Wired.

- Step 2** Configure the dual NIC—or verify the configuration—so that the following conditions are met:
- Both NICs are connected to the same network segment (in other words, both are connected to the same Layer 3 subnet and the same Layer 2 Ethernet broadcast domain).
 - Both share the same IP address.
 - Both are set up for AFT or for NFT. Refer to the NIC-configuration utility Help.
- Step 3** Write down the MAC address that now applies to both NICs. You will need it when you obtain license files in the “[Obtaining Cisco Unity License Files](#)” section on page 5-4.
- Step 4** Restart the Cisco Unity server for any changes to take effect.

Obtaining Cisco Unity License Files

License files, which enable the features purchased by the customer, are required for installing Cisco Unity software, for some upgrades, and for adding or changing licensed features. You obtain the license files by completing registration information on Cisco.com.

Shortly after registration, Cisco e-mails the license files. The e-mail from Cisco contains instructions on how to save and store the files. The Cisco Unity installation guide later provides specific instructions on the use of the license files. (For more information on licensing, refer to *White Paper: Licensing for Cisco Unity* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpaper/licenses.htm.)



Note

Install the license files only on the primary server.

The following information is required during registration:

- The MAC address (physical address) for the network interface card (NIC) in the Cisco Unity server.
- The product authorization key (PAK), which appears on the sticker located on the front of the sleeve for Cisco Unity DVD 1 or CD 1.

If the server contains a dual NIC and you configured it for fault tolerance by using the procedure in the “Configuring a Dual NIC in the Cisco Unity Server” section on page 5-2, you already have the MAC address. Skip to the “To Register and Obtain the License Files” procedure on page 5-5.

If the server contains one NIC or if the server contains a dual NIC that you did not configure for fault tolerance, do the following two procedures in the order listed.

To Get the MAC Address of the Cisco Unity Server When the Server Contains One NIC or an Un teamed Dual NIC

-
- Step 1** On the server on which Cisco Unity will be installed, on the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 2** In the Command Prompt window, enter **ipconfig /all**, and press **Enter**.
- Step 3** Write down the value of Physical Address, excluding the hyphens, or save it to a file that you can access during online registration. (For example, if the physical address is 00-A1-B2-C3-D4-E5, record 00A1B2C3D4E5.)
- If the server contains more than one NIC, one value will appear for each NIC. Write down the value for the NIC that you will use to connect the Cisco Unity server to the network.
- Step 4** Close the Command Prompt window.
-

To Register and Obtain the License Files

-
- Step 1** Browse to the applicable registration site (URLs are case sensitive):

Registered user on Cisco.com	http://www.cisco.com/go/license
Not a registered user on Cisco.com	http://www.cisco.com/go/license/public

- Step 2** Enter the PAK or software serial number, and click **Submit**.
- Step 3** Follow the on-screen prompts.
- Step 4** Shortly after registration, you will receive an e-mail with the Cisco Unity license files.
- If license files are lost, it can take up to one business day to get another copy.
-

If you do not receive the license files within 1 hour or to get another copy of a license file, call the Cisco Technical Assistance Center (TAC) and ask for the Licensing Team:

In the U.S.	800 553-2447
Outside the U.S.	For your local Cisco TAC phone number, refer to the website http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml .

Or send e-mail to licensing@cisco.com.

You will need to provide information to verify Cisco Unity ownership—for example, the purchase order number or the PAK (which appears on the sticker located on the front of the sleeve for Cisco Unity DVD 1 or CD 1).

**Note**

Cisco Unity software comes with a default license file that has a minimal number of settings. The license file allows installation of a Cisco Unity demonstration system. For information and instructions on installing a demonstration system, refer to the “Cisco Unity Demonstration System” section of the Cisco Unity release notes.

Running the Cisco Unity System Preparation Assistant

The Cisco Unity System Preparation Assistant is a program that helps customize the platform for Cisco Unity by checking for and installing Windows components, Microsoft service packs and updates, and other software required by Cisco Unity. For a detailed list, refer to *Components and Software Installed by the Cisco Unity Platform Configuration Discs and the Cisco Unity System Preparation Assistant* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/pcd/pcd_inst.htm.

**Caution**

Do not run the Cisco Unity System Preparation Assistant remotely by using Windows Terminal Services or other remote-access applications, or the installation of required software may fail.

To Run the Cisco Unity System Preparation Assistant

- Step 1** Log on to Windows by using an account that is a member of the local Administrators group.
- Step 2** On Cisco Unity Service Packs CD 1, browse to the **Cuspa** directory, and double-click **Cuspa.vbs**.
- Step 3** If prompted, double-click the language of your choice to continue the installation.
- Step 4** On the Welcome screen, click **Next**.
- Step 5** On the Cisco Unity Server Characteristics page, set the following fields:

Configuration	Click Voice Messaging Only .
Failover	Check the This Is a Primary or Secondary Failover Server check box. The assistant uses the information to determine that the system requires SQL Server.
Number of Ports	Enter the number of voice ports that you are connecting with the Cisco Unity server.

- Step 6** Click **Next**. The assistant lists the components and indicates whether or not they are installed.
- Step 7** Follow the prompts to install any missing components until you are prompted to install the data store.
If a Microsoft AutoMenu window appears when the assistant is installing an application, close the window and allow the assistant to continue.

- Step 8** Install SQL Server in the location you made note of in the “[Determining the Drive Locations for Files on the Cisco Unity Server](#)” section on page 2-4:
- a. In the Welcome dialog box, click **Next**.
 - b. In the Computer Name dialog box, click **Next** to accept the default setting **Local Computer**.
 - c. In the Installation Selection dialog box, click **Next** to accept the default setting **Create a New Instance of SQL Server, or Install Client Tools**.
 - d. Follow the on-screen prompts until the CD Key dialog box appears.
 - e. Enter the key for Cisco Unity Data Store 2000 from the sticker located on the CD sleeve, and click **Next**.
 - f. In the Installation Definition dialog box, click **Next** to accept the default setting **Server and Client Tools**.
 - g. In the Instance Name dialog box, check the **Default** check box.
 - h. Click **Next**.
 - i. In the Setup Type dialog box, click **Typical**.
 - j. Under Destination Folder, next to Program Files, click **Browse** and specify the location for binaries that you made note of in the “[Determining the Drive Locations for Files on the Cisco Unity Server](#)” section on page 2-4.
 - k. Under Destination Folder, next to Data Files, click **Browse** and specify the location for databases that you made note of in the “[Determining the Drive Locations for Files on the Cisco Unity Server](#)” section on page 2-4.
 - l. Click **Next**.
 - m. At the top of the Services Accounts dialog box, click **Use the Same Account for Each Service**.
 - n. Under Service Settings, click **Use the Local System Account**.
 - o. Click **Next**.
 - p. In the Authentication Mode dialog box, we recommend that you click **Windows Authentication Mode**.

If you click Mixed Mode—which is supported but is less secure—under Add Password for the SA Login, enter and confirm a password for the SQL Server system administrator logon.
 - q. Click **Next**.
 - r. In the Start Copying Files dialog box, click **Next**.
 - s. In the Choose Licensing Mode dialog box, click **Processor License For**, and specify the number of processors in the Cisco Unity server.
 - t. Click **Continue**.
 - u. If you are prompted about shutdown tasks before continuing with the installation, click **Next**.
 - v. Click **Finish**.
 - w. Skip to [Step 9](#).
- Step 9** When SQL Server installation is complete, continue following the on-screen prompts in the assistant to complete the platform customization.
- Step 10** Install SQL Server Service Pack 3a:
- a. On the Welcome screen, click **Next**.
 - b. Follow the on-screen prompts until you are prompted to choose the authentication mode.

- c. Choose Windows authentication, and click **Next**.
- d. If the SA Password Warning dialog box appears, enter and confirm the password, and click **Next**.
- e. Check the **Upgrade Microsoft Search and Apply SQL Server 2000 SP3 [Required]** check box, and click **Continue**. (Do not check the Enable Cross-Database Ownership Chaining for All Databases [Not Recommended] check box.)
- f. Follow the on-screen prompts to continue.
- g. If you are prompted about shutdown tasks before continuing with the installation, click **Next**.
- h. Click **Finish** to begin installing components.
- i. When the Setup message appears, click **OK**.
- j. Click **Finish** to restart the server.
- k. Skip to [Step 11](#).

Step 11 Follow the on-screen prompts.

Step 12 When the Cisco Unity System Preparation Assistant has completed, click **Finish**.



Caution

When the Cisco Unity System Preparation Assistant installed Internet Explorer, it also automatically installed the file WScript.exe. Do not remove WScript.exe, or the Cisco Unity Setup program will fail later in the installation process.

Changing Folder Settings in Windows Explorer

You change folder settings so that all files and folders—including system files—are visible in Windows Explorer during Cisco Unity troubleshooting.

If you installed Windows 2000 Server from the Platform Configuration discs that are shipped with a Cisco Unity server purchased from Cisco, all files and folders are already visible in Windows Explorer.



Note

If you do not do the following procedure now, Cisco TAC may ask you to do it later.

To Change Folder Settings in Windows Explorer

- Step 1** On the Windows desktop, double-click **My Computer**.
- Step 2** On the Tools menu, click **Folder Options**.
- Step 3** Click the **View** tab.
- Step 4** Click **Show Hidden Files and Folders**.
- Step 5** Uncheck the **Hide File Extensions for Known File Types** check box.
- Step 6** Uncheck the **Hide Protected Operating System Files** check box, and click **Yes** to confirm.
- Step 7** Click **Apply**.

- Step 8** Click **Like Current Folder**, and click **Yes** to confirm.
- Step 9** Click **OK**.
-

Installing the Latest Microsoft Service Packs and Updates for Windows, Internet Explorer, and SQL Server 2000

Install the latest Microsoft service packs (if any) and updates for Windows 2000 Server or Windows Server 2003, for Internet Explorer, and for SQL Server 2000 that are recommended for use with Cisco Unity. These are the service packs and updates that you downloaded in the “[Downloading Software for the Installation](#)” section on page 2-2.



Caution

If the Cisco Unity server is running Windows Server 2003, you must install the update associated with Microsoft Knowledge Base article 824330, or Cisco Unity will not function properly.

Some Microsoft updates can be installed only after a prerequisite service pack has been installed. Install any recommended service packs before you install updates.

Exchange software is not installed, so you cannot install Exchange service packs and updates yet.

To Install the Latest Microsoft Service Packs for Windows, Internet Explorer, and SQL Server 2000

Follow the instructions that you printed or downloaded when you downloaded the service packs.

To Install the Latest Microsoft Updates for Windows and SQL Server 2000

- Step 1** Insert the Cisco Unity Post-Install disc in the CD-ROM drive.
- Step 2** Browse to each of the applicable directories and install the correct language version of each update: English (ENU), French (FRA), German (DEU), or Japanese (JPN). (For example, if the French version of Windows 2000 Server is installed on the Cisco Unity server, install the French version of any Windows 2000 Server updates.)
- To speed the installation, you may want to:
- Install each update at a command prompt by using the /z option, so you do not have to restart the computer after installing each update.
 - Install each update at a command prompt by using the /m option, so the update installs without displaying any dialog boxes.
 - Create a batch file that installs all of the updates at once.
- Step 3** Restart the Cisco Unity server.
-

Disabling the Found New Hardware Wizard for the Voice Cards


Note

If the Cisco Unity server does not contain voice cards, skip this section.

In the following cases, the Found New Hardware wizard may appear each time the server is restarted and report that the cards are new hardware, even though the cards are properly installed and configured:

- The operating system was installed by using the Platform Configuration discs.
- The operating system was installed by using the manufacturer's guided system-setup utility before the cards were installed.
- New cards were added to an existing server.

Do the following procedure to prevent the Found New Hardware wizard from reporting the cards as new hardware. The procedure will not prevent the Found New Hardware wizard from finding and reporting other new hardware.

To Disable the Found New Hardware Wizard for the Voice Cards

-
- Step 1** On the Found New Hardware wizard Welcome page, click **Next**. (After the server is restarted, the Found New Hardware wizard Welcome page is displayed along with the PCI Device Installing dialog.)
- Step 2** On the Install Hardware Device Drivers page, click **Search for a Suitable Driver for My Device (Recommended)**, and click **Next**.
- Step 3** On the Locate Driver Files page, check the **Floppy Disk Drives** and **CD-ROM Drives** check boxes, and click **Next**.
- Step 4** On the Driver Files Search Result page, click **Disable the Device**, and click **Finish**. Do not choose to skip driver installation of this device, or the Found New Hardware wizard will continue to appear each time the server is restarted.
- Step 5** Repeat [Step 2](#) through [Step 4](#) for each instance of the Found New Hardware wizard (for each card, as applicable).

Note that doing this procedure does not prevent a card from being displayed as an unknown PCI device when viewed in the Windows 2000 Device Manager. The warning that the device drivers are not installed also will continue to be displayed. This is expected behavior, and does not indicate a problem with the card or with the server.

Installing Virus-Scanning Software (Optional)

For information on supported virus-scanning software, refer to *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm.

Follow the manufacturer instructions to install the virus-scanning software.

Note that scanning individual Exchange mailboxes can affect the performance of Cisco Unity.

**Caution**

Do not configure virus-scanning software to block WAV attachments, or voice messages will be stripped of their recordings.

Installing and Configuring Cisco Security Agent for Cisco Unity (Optional)

Cisco Security Agent for Cisco Unity is available on Cisco.com. For information on how to download it, install it on the Cisco Unity server, and configure it, refer to *Release Notes for Cisco Security Agent for Cisco Unity* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Connecting the Cisco Unity Server to the Network

To Connect the Cisco Unity Server to the Network

Attach the network cable(s) to the Cisco Unity server.

If the server contains a dual NIC, ensure that you connect the cable to the primary NIC, if you configured the dual NIC for AFT or NFT, or to the NIC that is enabled.

Configuring TCP/IP Properties

The Cisco Unity server must have an IP address and must also have the IP address of a DNS server. Do the procedure in this section to specify IP addresses for the servers.

When selecting an IP address for the Cisco Unity server, note the following considerations:

- Do not assign an externally routable IP address. Doing so can expose the Cisco Unity server to unwanted intrusion from the Internet, even when the server is hardened.
- Do not select an address that puts the Cisco Unity server on the opposite side of a firewall from:
 - The Exchange server that Cisco Unity connects with.
 - Any Exchange server that homes Cisco Unity subscriber mailboxes.
 - The domain controller/global catalog server that Cisco Unity accesses.

To Configure TCP/IP Properties

- Step 1** On the Windows Start menu, click **Settings > Control Panel > Network and Dial-Up Connections > Local Area Connection**.
- Step 2** Click **Properties**.
- Step 3** In the Components Checked Are Used by This Connection list, check the **Internet Protocol (TCP/IP)** check box.

- Step 4** Click **Internet Protocol (TCP/IP)** (but do not uncheck the check box), and click **Properties**.
 - Step 5** Enter IP addresses for the Cisco Unity server and for the preferred and alternate DNS servers (for more information, refer to Windows Help).
 - Step 6** Click **OK**
 - Step 7** Restart the server.
-

Verifying the IP Address and the Network Connection

To Verify the IP Address and the Network Connection

- Step 1** On the Windows Start menu, click **Programs > Accessories > Command Prompt**.
 - Step 2** In the Command Prompt window, enter **ipconfig /all**, and press **Enter**.
 - Step 3** Verify the IP address of the Cisco Unity server.
 - Step 4** Find the IP address of a router or server on the same network segment as the Cisco Unity server.
If no routers or servers are listed, either you did not specify a default gateway when you assigned an IP address in the [“Configuring TCP/IP Properties”](#) section on page 5-11, or the Cisco Unity server is not connected to the network.
 - Step 5** Ping the router or other server whose IP address you found in [Step 4](#). In the Command Prompt window, enter **ping <IP address>**, and press **Enter**.
If the device sends a reply, the Cisco Unity server has a valid IP address.
If the device does not reply, there may be a variety of causes. Some of the most common problems include:
 - The assigned IP address conflicts with the IP address of another computer on the network.
 - The subnet mask is incorrect.
 Verify the network settings. If needed, troubleshoot any problem as you would a network connectivity problem.
-

Disabling Virus-Scanning and Cisco Security Agent Services



Note

If the system is not using virus-scanning software or Cisco Security Agent for Cisco Unity, skip this section.

You disable virus-scanning and Cisco Security Agent services on the server so that they do not slow down the installation of software or cause the installations to fail. The Cisco Unity installation guide alerts you when to re-enable the services after all of the installation procedures that can be affected are complete.

To Disable and Stop Virus-Scanning and Cisco Security Agent Services

- Step 1** Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 3** Disable and stop each virus-scanning service and the Cisco Security Agent service:
- In the right pane, double-click the service.
 - On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
 - Click **Stop** to stop the service immediately.
 - Click **OK** to close the Properties dialog box.
- Step 4** When the services have been disabled, close the Services MMC.
-

Adding the Cisco Unity Server to an Existing Domain

The Cisco Unity server must be a member server in an existing domain. Cisco Unity interactions with the message store do not allow the server to be in a workgroup.

Add the primary and secondary Cisco Unity servers to the same domain.

We recommend that you install the Cisco Unity server in the same domain as the Exchange server that homes the Cisco Unity subscribers.

To Add the Cisco Unity Server to an Existing Domain

- Step 1** Log on to the Cisco Unity server by using an account that is a member of the local Administrators group.
- Step 2** On the Windows Start menu, click **Settings > Control Panel > System**.
- Step 3** Click the **Network Identification** tab.
- Step 4** Click **Properties**.
- Step 5** In the Identification Changes dialog box, click **Domain**, and enter the name of the domain that you want to join.
- Add the primary and secondary Cisco Unity servers to the same domain.
- Step 6** Click **OK**.
- Step 7** In the Domain Username and Password dialog box, enter the name and password of an account that has permission to add computers to the domain.
- Step 8** Click **OK** three times.
- Step 9** Click **Yes** to restart the server.
-

Resetting the Account That SQL Server Services Log On As

When you installed SQL Server, you set the services to use the local system account because the Cisco Unity server was not connected to the network. On both the primary and secondary servers for Cisco Unity failover, you must reset the account that the MSSQLServer and SQLServerAgent services log on as. The account must be a domain account and must:

- Have the right to log on as a service.
- Be a member of the local Administrators group.

To Reset the Account that SQL Server Services Log on As

- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 2** Do the following eight substeps for each of the two services, MSSQLServer and SQLServerAgent:
- a. In the right pane, double-click <Name of service>.
 - b. Click the **Log On** tab.
 - c. Click **This Account**.
 - d. Click **Browse**.
 - e. In the Select User dialog box, in the Look In list, click the name of the domain to which the Cisco Unity server belongs.
 - f. Double-click the name of the account to use. You must use the same account on both the primary and secondary Cisco Unity servers.
 - g. Enter and confirm the password.
 - h. Click **OK**.
- Step 3** When you are done setting both accounts, close the Services window.
-



Setting Up Exchange

In this chapter, you do the following tasks in the order listed:



Note

If you are installing the secondary Cisco Unity server now, skip Task 1.

1. Determine the Exchange server that Cisco Unity will connect with, known as the partner Exchange server. See the [“Determining the Partner Exchange Server”](#) section on page 6-2.
2. Install Exchange administration software on the Cisco Unity server. See the [“Installing Exchange Administration Software on the Cisco Unity Server”](#) section on page 6-2.
3. Install the latest Exchange service pack (if any) and updates that are recommended for use with Cisco Unity. See the [“Installing the Latest Exchange Service Pack and Updates”](#) section on page 6-5.



Note

If you are installing the secondary Cisco Unity server now, skip Task 4.

4. Extend the Active Directory schema for Cisco Unity. See the [“Extending the Active Directory Schema for Cisco Unity”](#) section on page 6-6.



Note

If you are installing the secondary Cisco Unity server now, skip Task 5.

5. Create Active Directory organizational units for users and distribution lists, and a mailbox store, if applicable. See the [“Creating Organizational Units and a Mailbox Store”](#) section on page 6-7.

When you are finished with this chapter, return to the [“Overview of Mandatory Tasks for Installing Cisco Unity”](#) chapter to continue installing the Cisco Unity system.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Determining the Partner Exchange Server

During configuration of the Cisco Unity software, you will be prompted to select an Exchange server for Cisco Unity to connect with. The server is known as the partner Exchange server, or the partner server. You decide now which server you will use as the partner server, based on the following information; you specify the partner server later in the installation process.

When all Cisco Unity subscriber mailboxes will be homed on the same Exchange server, use that server as the partner server.

When Cisco Unity subscriber mailboxes will be homed on more than one Exchange server, consider the following general guidelines for deciding which server to use as the partner server:

- All voice messages from outside callers pass through the partner server on their way to user mailboxes. Use an Exchange server based on its ability to handle the additional traffic.
- When Exchange is configured for active/active or active/passive clustering, use either an Exchange server outside the cluster or the Exchange virtual server in the cluster.



Caution

When Windows Server 2003 is installed on the Cisco Unity server, you must use Exchange 2003.

Installing Exchange Administration Software on the Cisco Unity Server

The version of administration software that you install on the Cisco Unity server must be the same as the version of Exchange installed on the separate partner Exchange server.

See the applicable section, depending on the Exchange version on the partner server:

- [Installing Exchange 2003 Administration Software, page 6-2](#)
- [Installing Exchange 2000 Administration Software, page 6-4](#)

Installing Exchange 2003 Administration Software



Note

Cisco assumes that the Exchange environment is already set up and working before the Cisco Unity system is installed.

When Exchange 2003 is installed on the partner server, you install Exchange 2003 administration software on the Cisco Unity server because it includes the Microsoft messaging API (MAPI). MAPI is the application programming interface that Cisco Unity uses to communicate with Exchange for addressing, sending, and retrieving messages.



Caution

Do not install Exchange Messaging and Collaboration Services on the Cisco Unity server.

Later in the installation process, you specify the partner Exchange server that Cisco Unity connects with. Do the following two procedures in the order listed.

To Install Exchange 2003 Administration Software on the Cisco Unity Server

-
- Step 1** On the Cisco Unity server, insert the Exchange Server 2003 disc in the CD-ROM drive.
If the disc does not run automatically, browse to the root directory, and double-click **Setup.exe**.
- Step 2** Click **Exchange Deployment Tools**.
- Step 3** Click **Install Exchange System Management Tools Only**.
- Step 4** On the Install Exchange System Management Tools Only page, scroll down to Step 4 and click **Run Setup Now**.



Note In early editions of Exchange 2003, Step 3 on the Install Exchange System Management Tools Only page incorrectly listed Windows Server 2003 Administration Tools Pack as required when the operating system is Windows 2000 Server. In later editions of Exchange 2003, this requirement was removed from Help, as explained in Microsoft Knowledge Base article 826966.

- Step 5** In the Welcome to Microsoft Exchange Installation wizard, click **Next**.
- Step 6** In the License Agreement dialog box, click **I Agree**, and click **Next**.
- Step 7** In the Component Selection dialog box, in the Action column, set the actions for the following three components:

Microsoft Exchange 2003	Change the action to Custom .
Microsoft Exchange Messaging and Collaboration Services	Change the action to None .
Microsoft Exchange System Management Tools	Leave the action as Install .

- Step 8** Click **Next**.
- Step 9** Follow the on-screen prompts to complete the installation.
- Step 10** Restart the server.

To Install Exchange 2003 Service Pack 1 on the Cisco Unity Server

-
- Step 1** On Cisco Unity Service Packs CD 2, browse to the directory **Exchange_2003_SP1\Setup\I386**, and double-click **Update.exe**.
- Step 2** Follow the on-screen prompts to complete the installation.
- Step 3** Restart the server.
- Step 4** If you have not already done so, repeat this procedure on the partner Exchange server and on every Exchange 2003 server on which Cisco Unity subscriber mailboxes are homed.
-

Installing Exchange 2000 Administration Software


Note

Cisco assumes that the Exchange environment is already set up and working before the Cisco Unity system is installed.

When Exchange 2000 is installed on the partner server, you install Exchange 2000 administration software on the Cisco Unity server because it includes the Microsoft messaging API (MAPI). MAPI is the application programming interface that Cisco Unity uses to communicate with Exchange for addressing, sending, and retrieving messages.

Later in the installation process, you specify the partner Exchange server that Cisco Unity connects with. Do the following four procedures in the order listed.

To Install Exchange 2000 Administration Software on the Cisco Unity Server

- Step 1** On the Cisco Unity server, insert the Cisco Unity Message Store 2000 disc in the CD-ROM drive. If the disc does not run automatically, browse to the root directory, and double-click **Launch.exe**.
- Step 2** Click **Exchange Server Setup**.
- Step 3** Follow the on-screen prompts until the Product Identification dialog box appears.
- Step 4** Enter the key for Cisco Unity Message Store 2000 from the sticker located on the CD sleeve, and click **Next**.
- Step 5** In the Component Selection dialog box, in the Action column, set the actions for the following three components:

Microsoft Exchange 2000	Change the action to Custom .
Microsoft Exchange Messaging and Collaboration Services	Change the action to None .
Microsoft Exchange System Management Tools	Leave the action as Install .

- Step 6** Click **Next**.
- Step 7** Follow the on-screen prompts to complete the installation.
- Step 8** Restart the server.

Exchange 2000 Service Pack 3 and the Exchange 2000 Server Post-Service Pack 3 Rollup that is described in Microsoft Knowledge Base article 824282 resolve an intermittent problem with message notification.


Note

If Service Pack 3 and the rollup are not installed, Exchange 2000 Server sends extra UDP packets to ports on the Cisco Unity server that are not listening for packets. Such activity is seen by intrusion-detection systems as port scans or attacks.

To Install Exchange 2000 Service Pack 3

- Step 1** On Cisco Unity Service Packs CD 2, browse to the directory **Exchange_2000_SP3\Setup\I386**, and double-click **Update.exe**.
 - Step 2** Follow the on-screen prompts to complete the installation.
 - Step 3** Restart the server.
 - Step 4** If you have not already done so, repeat this procedure on the partner Exchange server and on every Exchange 2000 server on which Cisco Unity subscriber mailboxes are homed.
-

To Install the Exchange 2000 Post-Service Pack 3 Rollup

- Step 1** On the Cisco Unity Post-Install CD, browse to the directory **Exchange_2000_Post_SP3_Rollup\Setup\I386**, and double-click **Update.exe**.
 - Step 2** Follow the on-screen prompts to complete the installation.
 - Step 3** Restart the server.
 - Step 4** If you have not already done so, repeat this procedure on the partner Exchange server and on every Exchange 2000 server on which Cisco Unity subscriber mailboxes are homed.
-

In the next procedure, you disable the Windows License Logging service on all Exchange servers on which Cisco Unity subscriber mailboxes are homed to prevent Exchange 2000 license errors in the event log. (If the service is not disabled in a Cisco Unity Voice Messaging configuration with Exchange 2000 as the message store, the service logs errors in the event log about Exchange 2000 being out of licenses, even though Microsoft client access licenses (CALs) are not required.)

To Disable the License Logging Service

- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 2** In the right pane, right-click **License Logging Service**, and click **Properties**.
 - Step 3** On the General tab, click **Stop**.
 - Step 4** Under Startup Type, click **Disabled**.
 - Step 5** Click **OK**.
 - Step 6** Close the Services MMC.
-

Installing the Latest Exchange Service Pack and Updates

Install the latest Exchange service pack (if any) and updates that are recommended for use with Cisco Unity. These are the service pack and updates that you downloaded in the “[Downloading Software for the Installation](#)” section on page 2-2.

Some Exchange updates can be installed only after a prerequisite service pack has been installed. Install the service pack, if any, before you install updates.

To Install the Latest Exchange Service Pack

Follow the instructions that you printed or downloaded when you downloaded the service pack.

To Install the Latest Exchange Updates

- Step 1** Insert the Cisco Unity Post-Install disc in the CD-ROM drive.
- Step 2** Browse to each of the applicable directories and install the correct language version of each update: English (ENU), French (FRA), German (DEU), or Japanese (JPN). (For example, if the French version of Exchange 2000 administration software is installed on the Cisco Unity server, install the French version of any Exchange 2000 updates.)
- To speed the installation, you may want to:
- Install each update at a command prompt by using the /z option, so you do not have to restart the computer after installing each update.
 - Install each update at a command prompt by using the /m option, so the update installs without displaying any dialog boxes.
 - Create a batch file that installs all of the updates at once.
- Step 3** Restart the Cisco Unity server.
-

Extending the Active Directory Schema for Cisco Unity

Several changes need to be made to the Active Directory schema for Cisco Unity to work properly. To see the changes that the schema update program makes, browse to the directory SchemaLdifScripts on Cisco Unity DVD 1 or CD 1, and view the file Avdirmonex2k.ldf.

Changes to the Active Directory schema may take 15 minutes or more to replicate throughout the forest. The changes must finish replicating before you can install Cisco Unity.

To Extend the Active Directory Schema for Cisco Unity

- Step 1** Confirm that all domain controllers are on line. (The Active Directory schema extensions replicate only when all domain controllers are on line.)
- Step 2** On the computer that has the schema master role (typically the first DC/GC in the forest), log on to Windows as a user who is a member of the Schema Admins group.
- Step 3** On Cisco Unity DVD 1 or CD 1, browse to the directory **ADSchemaSetup**, and double-click **ADSchemaSetup.exe**.
- Step 4** In the Active Directory Schema Setup dialog box, check the **Exchange 2000 or Exchange 2003 Directory Monitor** check box.
- Step 5** If you plan to use VPIM Networking or Cisco Unity Bridge Networking, check the applicable check boxes.

- Step 6** Click **OK**.
- Step 7** When the schema extension has finished, Ldif.log and Ldif.err files are saved to the desktop. View the contents of the files to confirm that the extension completed successfully.
-

Creating Organizational Units and a Mailbox Store

Users and distribution lists are created in locations that you specify. If you want users and distribution lists to be created in custom organizational units (OUs), create the OUs now. Both OUs need to be in the same domain, but they do not need to be in the same domain as the Cisco Unity server. For information on creating OUs, refer to Active Directory Users and Computers Help.

You also have the option to create a custom mailbox store as the default for subscribers that are added through the Cisco Unity Administrator or that are imported from a CSV file. For information on creating a custom mailbox store, refer to Exchange System Manager Help. (Later in the installation process, you configure Cisco Unity to use the mailbox store.)

You must use the same custom OUs and mailbox stores for the primary and secondary Cisco Unity servers.



Creating Accounts for the Installation and Setting Rights and Permissions

In this chapter, you do the following tasks in the order listed:



Note

If you are installing the secondary Cisco Unity server now, skip Task 1.

1. Familiarize yourself with the domain accounts you will create in Task 2. See the [“About the Accounts Required for the Cisco Unity Installation”](#) section on page 7-2.



Note

If you are installing the secondary Cisco Unity server now, skip Task 2.

2. Create the applicable domain accounts that are needed to install Cisco Unity. See the [“Creating the Accounts Required for the Cisco Unity Installation”](#) section on page 7-3.
3. *If you created a Cisco Unity administration account in Task 2.:* Add the account to the local Administrators group. See the [“Adding the Cisco Unity Administration Account to the Local Administrators Group”](#) section on page 7-3.
4. Set rights and permissions for the accounts that you created in Task 2. See the [“Setting Rights and Permissions with the Cisco Unity Permissions Wizard”](#) section on page 7-4.



Note

If you are installing the secondary Cisco Unity server now, skip Task 5.

5. Set Exchange permissions. See the [“Setting Required Exchange Permissions”](#) section on page 7-8.

When you are finished with this chapter, return to the [“Overview of Mandatory Tasks for Installing Cisco Unity”](#) system to continue installing the Cisco Unity system.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

About the Accounts Required for the Cisco Unity Installation

This section describes the following domain accounts that are needed for the Cisco Unity installation:

- [The Account Used to Install Cisco Unity, page 7-2](#)
- [The Account Used to Access the Cisco Unity Administrator, page 7-2](#)
- [The Accounts That Cisco Unity Services Log On As, page 7-2](#)

**Note**

The same accounts are required for installing a new Cisco Unity 4.0(x) system and for upgrading from previous versions of Cisco Unity.

The Account Used to Install Cisco Unity

During installation, Cisco Unity creates a number of Cisco Unity objects in Active Directory and in Exchange, so the account with which you log on to Windows to install Cisco Unity must have proper user rights and permissions to perform the necessary operations.

If you are installing more than one Cisco Unity server in a site—including setting up failover—you can use the same account to install Cisco Unity software on all of the servers.

The Account Used to Access the Cisco Unity Administrator

When you install Cisco Unity, you are prompted to choose the Windows domain account that you want to use to access the Cisco Unity Administrator (the website used to perform most administration tasks). During installation, the domain account is automatically associated with a Cisco Unity subscriber whose class of service allows Cisco Unity Administrator access. (Later you can create additional Cisco Unity subscribers who also can access the Cisco Unity Administrator.)

By default, the Cisco Unity administration account is the installation account. If you prefer to use an account other than the installation account to be the first Cisco Unity administration account, create an additional domain account for that purpose.

The Cisco Unity administration account must be a member of the local Administrators group. A procedure later in this chapter explains how to add the account to that group.

The Accounts That Cisco Unity Services Log On As

During Cisco Unity installation, you are prompted to choose three domain accounts that Cisco Unity services log on as:

- The account that Cisco Unity directory services log on as. These services keep subscriber data in the directory synchronized with subscriber data in the Cisco Unity SQL Server database.
- The account that Cisco Unity message store services log on as. These services allow subscribers to send and receive voice messages by using the telephone user interface.
- The account that local services log on as. By default, local Cisco Unity services log on as the Local System account. We recommend that you not change this.

The permissions required by the directory services account conflict with the permissions required by the message store services account, so you must create separate accounts for the two types of services.

Creating the Accounts Required for the Cisco Unity Installation

To Create Domain Accounts for Cisco Unity Installation, Administration, and Services

- Step 1** On the Cisco Unity server, log on to Windows by using an account that is a member of the Domain Admins group.
- Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > Active Directory Users and Computers** or click **Programs > Administrative Tools > Active Directory Users and Computers**.
- Step 3** In the left pane, expand the domain, right-click **Users** or the organizational unit where you want to create the installation account, and click **New > User**.
- Step 4** Follow the on-screen prompts to create the installation account. Creating an Exchange mailbox is optional.

We suggest that you use the following names for the accounts:

Installation	UnityInstall
Administration	UnityAdmin
Account that Cisco Unity directory services log on as (directory services account)	UnityDirSvc
Account that Cisco Unity message store services log on as (message store services account)	UnityMsgStoreSvc

- Step 5** Repeat [Step 3](#) and [Step 4](#) to create the Cisco Unity administration account, the directory services account, and the message store services account.
- Ensure that for the accounts that Cisco Unity services log on as, the password will never expire. If the password expires, Cisco Unity will stop working the next time the server is restarted.
- Step 6** Close Active Directory Users and Computers.

Adding the Cisco Unity Administration Account to the Local Administrators Group



Note

If you did not create a Cisco Unity administration account in the [“Creating the Accounts Required for the Cisco Unity Installation”](#) section on page 7-3, skip this section.

Add the Cisco Unity administration account to the local Administrators group on the primary and secondary Cisco Unity servers.

To Add the Cisco Unity Administration Account to the Local Administrators Group

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Computer Management**.

- Step 2** In the left pane of the Computer Management MMC, expand **System Tools > Local Users and Groups**.
- Step 3** In the left pane, click **Groups**.
- Step 4** In the right pane, double-click **Administrators**.
- Step 5** In the Administrators Properties dialog box, click **Add**.
- Step 6** In the Select Users or Groups dialog box, in the Look In list, click the name of the domain to which the Cisco Unity server belongs.
- Step 7** In the top list, double-click the name of the Cisco Unity administration account. The name appears in the bottom list.
- Step 8** Click **OK** to close the Select Users or Groups dialog box.
- Step 9** Click **OK** to close the Administrators Properties dialog box.
- Step 10** Close the Computer Management MMC.
-

Setting Rights and Permissions with the Cisco Unity Permissions Wizard

The procedure in this section sets the permissions that Cisco Unity requires for:

- The account that you will use to install Cisco Unity.
- The two accounts that Cisco Unity directory and message store services will log on as.

In addition, you must set Exchange-specific permissions, as described in the [“Setting Required Exchange Permissions”](#) section on page 7-8.

You run the Permissions wizard on both the primary and secondary Cisco Unity servers.

The Permissions wizard will complete in under an hour, and possibly in just a few minutes.

Before you can run the Permissions wizard, the Active Directory schema must have been extended for Cisco Unity, which you should have done when you set up the message store (in the [“Extending the Active Directory Schema for Cisco Unity”](#) section on page 6-6).



Caution

Cisco Unity needs to be able to change properties of Active Directory users. The Permissions wizard grants the directory services account the right to change user accounts in the containers that you specify. Cisco Unity can change user accounts in those containers only if inheritance is enabled for the containers and for the users themselves. If you disable inheritance for any containers or groups that include Cisco Unity subscribers, or for any users who are subscribers, Cisco Unity (using the directory services account) will not be able to change properties for the affected users. In that case, you will need to either grant permissions to those users explicitly or re-enable inheritance by checking the Allow Inheritable Permissions from Parent to Propagate to This Object check box on the Security tab in the applicable Properties dialog box.

The following procedure grants the installation and services accounts the rights to act as a part of the operating system, to log on as a service, and to log on as a batch job, and does so in the local security policy. (For a complete list of the permissions set by Permissions Wizard, refer to the Permissions Wizard Help file PWHelpPermissionsSet_<language>.htm.)

To Run the Cisco Unity Permissions Wizard

-
- Step 1** If a domain security policy is in effect, confirm that the domain security policy does not deny the installation and services accounts the rights to act as a part of the operating system, to log on as a service, and to log on as a batch job.
- Step 2** Log on to the Cisco Unity server by using an account that:
- Is a member of the Domain Admins group in the domain in which the Cisco Unity server is being installed.
 - Is either an Exchange Full Administrator or a member of the Domain Admins group in the domain that contains all of the domains from which you want to import Cisco Unity subscribers.



Caution If you try to run the Permissions wizard by using an account that has less than the default permissions for a Domain Admin, the wizard may not be able to set all of the permissions required by the installation account and the services accounts. If the Permissions wizard cannot set all of the required permissions, either the Cisco Unity installation will fail or Cisco Unity will not run properly after it has been installed.

- Step 3** On Cisco Unity DVD 1 or CD 1, browse to the **Utilities\PermissionsWizard** directory, and run **PermissionsWizard.exe**.
- Step 4** On the Welcome to the Cisco Unity Permissions Wizard page, click **Microsoft Exchange 2000** or **Microsoft Exchange 2003**, depending on the version of Exchange installed on the partner Exchange server.
- If Windows Server 2003 is installed on the Cisco Unity server, **Microsoft Exchange 2003** is the only option available.
- Step 5** Click **Next**.
- Step 6** On the Installation Account page, click **Change**, and choose the account that you want to use to install Cisco Unity.
- Step 7** Click **Next**.
- Step 8** On the Directory Services Account page, click **Change**, and choose the account that you want Cisco Unity directory services to log on as.
- Step 9** Click **Next**.
- Step 10** On the Message Store Services Account page, click **Change**, and choose the account that you want Cisco Unity message store services to log on as.
- Step 11** Click **Next**.
- Step 12** Cisco Unity needs access to one or more Active Directory organizational units to create users (Cisco Unity subscribers) and groups (Cisco Unity distribution lists). On the Set Active Directory Containers for New Objects page, choose the following:
- The domain in which you want new users and groups to be created.
 - The organizational unit in which you want users to be created. This is where Cisco Unity Example Administrator will be created during Cisco Unity installation.
 - The organizational unit in which you want groups to be created.
- Step 13** Click **Next**.

Step 14 On the Objects the Cisco Unity Administrator Can Create page, check the check boxes for the objects you want to be able to create by using the Cisco Unity Administrator.

If you do not want to use the Cisco Unity Administrator to create new Active Directory users, contacts, and groups, you may choose not to grant the Cisco Unity directory services account the necessary rights to create each type of Active Directory object.

If you uncheck a check box next to an Active Directory object type, you will not be able to create the associated type of Cisco Unity object by using the Cisco Unity Administrator. You may only import existing objects into Cisco Unity. (For example, if you uncheck the Users check box, you will not be able to create new Cisco Unity subscribers by using the Cisco Unity Administrator. You will only be able to import existing Active Directory users to make them Cisco Unity subscribers.)

Step 15 Click **Next**.

Step 16 On the Set Active Directory Container for Location Objects page, choose the organizational unit in which you want Cisco Unity location objects to be created.

Step 17 Click **Next**.

Step 18 On the Set Active Directory Containers for Import page, choose the Active Directory containers from which you want to import users, contacts, and groups to make them Cisco Unity subscribers and public distribution lists. Note the following considerations:

- You must choose a container for the domain that includes the Cisco Unity server.
- Choose only one container for each domain. If you will want to import users and groups from more than one container in a domain, choose a common parent container that includes all of the containers from which you want to import. If the common parent is the domain itself, choose the domain.

Alternatively, if you want to choose multiple containers without choosing the common parent container, you can run the Permissions wizard more than once. Every time you run the Permissions wizard, choose the same options except on this page, where you choose a different container each time.

- If you are using Digital Networking to connect multiple Cisco Unity servers and if you will be importing users from the same container for every Cisco Unity server, choose that container. (For example, if CiscoUnityServer1 and CiscoUnityServer2 will both be importing users only from Container1, choose Container1.)

If you are using Digital Networking and if, for all of the Cisco Unity servers combined, you will be importing users from two or more containers, the Cisco Unity message store services account on each Cisco Unity server must be granted SendAs permission on every container from which users will be imported on every Cisco Unity server in the forest. (For example, if CiscoUnityServer1 will import users from Container1 and Container2, and if CiscoUnityServer2 will import users from Container3 and Container4, the Cisco Unity message store services account on each Cisco Unity server must have SendAs permission for all four containers.) On each Cisco Unity server, do one of the following, or identified subscriber messaging may not work between Cisco Unity servers:

- Choose all of the containers from which users will be imported by choosing a common parent container.
- Choose all of the containers from which users will be imported by running the Permissions wizard more than once.
- Use the same Active Directory account for the Cisco Unity message store services account as on every other Cisco Unity server in the forest.
- If you are using identified subscriber messaging for AMIS, the Cisco Unity Bridge, or VPIM, and if you will be importing contacts from the same container for every Cisco Unity server, choose that container. (For example, if CiscoUnityServer1 and CiscoUnityServer2 will both be importing contacts only from Container1, choose Container1.)

If you are using identified subscriber messaging for AMIS, the Bridge, or VPIM, and if, for all of the Cisco Unity servers combined, you will be importing contacts from two or more containers, the Cisco Unity message store services account on each Cisco Unity server must be granted SendAs permission on every container from which contacts will be imported on every Cisco Unity server in the forest. (For example, if CiscoUnityServer1 will import contacts from Container1 and Container2, and if CiscoUnityServer2 will import contacts from Container3 and Container4, the Cisco Unity message store services account on each Cisco Unity server must have SendAs permission for all four containers.) On each Cisco Unity server, do one of the following, or identified subscriber messaging may not work between Cisco Unity servers:

- Choose all of the containers from which contacts will be imported by choosing a common parent container.
- Choose all of the containers from which contacts will be imported by running the Permissions wizard more than once.
- Use the same Active Directory account for the Cisco Unity message store services account as on every other Cisco Unity server in the forest.

Step 19 Click **Next**.

Step 20 On the Choose Mailstores page, click **Next**. Cisco Unity subscribes will be homed in all of the available Exchange 2003 or Exchange 2000 mailstores.

Step 21 The Verify Permission Assignments page appears, listing the permissions that will be granted to each account. The information listed includes user rights, Active Directory rights, and membership in groups. Click **Next** to grant the listed permissions.

Step 22 If the Permissions wizard failed to grant one or more permissions, an error message appears that lists the number of permissions it was not able to grant. Click **OK**.

Step 23 To display a report listing the operations that succeeded and those that failed, if any, click **View Detailed Results**.

Note that in some cases, individual rights may be combined into a single entry. For example, the rights to read properties, write properties, list contents, read permissions, and modify permissions applied on Group objects are all included in the single entry “SUCCEDED granting Group read/modify rights.”

Step 24 If one or more permissions could not be granted, fix the problems, and run the Permissions wizard again.



Caution

If the Permissions wizard failed to set any permissions, either the Cisco Unity installation will fail or Cisco Unity will not run properly after it has been installed. You must successfully run the Permissions wizard before you can continue installing Cisco Unity.



Caution

An Active Directory right being granted by the Permissions wizard may conflict with an existing right on an Active Directory container. (For example, an account may be denied the right to create user objects in one of the containers selected during the Permissions wizard.) The log file will explain that a conflict has been found, but the Permissions wizard will not resolve the conflict. You must resolve the conflict and then rerun the Permissions wizard.

Step 25 Click **Finish**.

Step 26 If the account that you logged on with in [Step 2](#) is also the account that you want to use to install Cisco Unity (the account that you selected in [Step 6](#)), log off of Windows so the permissions set by the Permissions wizard will take effect.

Setting Required Exchange Permissions

In general, the Cisco Unity Permissions wizard does not set Exchange permissions, so they must be set manually. (The Permissions wizard does grant Send-As, Receive-As, and Administer Information Store permissions on Exchange 2003 or Exchange 2000 mailstores.)

The following Exchange permissions must be set for the Cisco Unity installation and services accounts:

Installation account	Exchange Administrator.
Cisco Unity directory services account	Exchange Administrator if you want to create Cisco Unity subscribers by using the Cisco Unity Administrator. Exchange View Only Administrator if you want to create Cisco Unity subscribers only by importing accounts from Active Directory.
Cisco Unity message store services account	Send-As, Receive-As, and Administer Information Store permissions on Exchange 2003 or Exchange 2000 mailstores (set by the Permissions wizard).

Do the following procedure for the installation account first, then for the directory services account. Note that you set Exchange permissions only on the primary Cisco Unity server.

To Grant Exchange Permissions to the Installation and Directory Services Accounts

- Step 1** Log on to the Cisco Unity server by using an account that is an Exchange Full Administrator.
- Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > System Manager**.
- Step 3** In the left pane of the Exchange System Manager MMC, right-click the organization name at the top of the tree control, and click **Delegate Control**.
- Step 4** On the Welcome to the Exchange Administration Delegation Wizard page, click **Next**.
- Step 5** In the Users or Groups dialog box, click **Add**.
- Step 6** In the Delegate Control dialog box, click **Browse**.
- Step 7** In the Select Users, Computers, or Groups dialog box, in the Look In list, click the name of the domain to which the Cisco Unity server belongs.
- Step 8** When you are granting permissions for the installation account, in the list of users, computers, and groups, double-click the name of the account.

When you are granting permissions for the Cisco Unity directory services account, in the list of users, computers, and groups, double-click the name of the account.

The Delegate Control dialog box reappears. The account you selected appears in the Group (Recommended) or User box.

Step 9 When you are setting permissions for the installation account, in the Role list, click **Exchange Administrator**.

When you are setting permissions for the Cisco Unity directory services account, in the Role list, click the applicable option:

Exchange Administrator	If you want to create Cisco Unity subscribers by using the Cisco Unity Administrator.
Exchange View Only Administrator	If you do not want to create Cisco Unity subscribers by using the Cisco Unity Administrator (meaning that you will create Cisco Unity subscribers only by importing accounts from Active Directory).

Step 10 Click **OK** to close the Delegate Control dialog box.

Step 11 Repeat [Step 5](#) through [Step 10](#) for the Cisco Unity directory services account.

Step 12 Click **Next**.

Step 13 Click **Finish**.

Step 14 Close the Exchange System Manager MMC.



Installing and Configuring Cisco Unity Software

In this chapter, you do the following tasks in the order listed:

1. Determine whether to set up Cisco Unity to use SSL. See the [“Determining Whether to Set Up Cisco Unity to Use SSL”](#) section on page 8-2.



Note

If you are installing the secondary Cisco Unity server now, skip Task 2.

2. *If you plan to set up Cisco Unity to use SSL and want to use the Microsoft Certificate Services available with Windows to issue your own certificate:* Install the Microsoft Certificate Services component. See the [“Installing the Microsoft Certificate Services Component”](#) section on page 8-3.
3. Use the Cisco Unity Installation and Configuration Assistant to install and configure Cisco Unity, and to set up the Cisco Personal Communications Assistant to use SSL. See the [“Installing and Configuring Cisco Unity Software”](#) section on page 8-3.
4. Install the Cisco Unity 4.0(5) service release, if available. See the [“Installing the Cisco Unity Service Release, If Available”](#) section on page 8-16.



Note

If you are installing the secondary Cisco Unity server now, skip Task 5.

5. Test the phone system integration. See the [“Testing the Phone System Integration”](#) section on page 8-16.
6. *If virus-scanning software is installed on the Cisco Unity server:* Exclude from scanning the directory in which Cisco Unity is installed. See the [“Excluding from Virus Scanning the Directory in Which Cisco Unity Is Installed”](#) section on page 8-16.
7. *If you are setting up Cisco Unity to use SSL:* Set up the Cisco Unity Administrator and Status Monitor to use SSL. See the [“Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL”](#) section on page 8-17.



Note

If you are installing the secondary Cisco Unity server now, skip Task 8.

8. Secure the Example Administrator account against toll fraud. See the [“Securing the Example Administrator Account Against Toll Fraud”](#) section on page 8-18.

9. Move SQL Server databases and transaction logs. See the [“Moving the Data Store Databases and Transaction Logs”](#) section on page 8-18.
10. *If virus-scanning software or Cisco Security Agent for Cisco Unity is installed on the Cisco Unity server:* Re-enable virus-scanning services and the Cisco Security Agent service for Cisco Unity. See the [“Re-enabling Virus-Scanning and Cisco Security Agent Services”](#) section on page 8-21.
11. Secure Cisco Unity and the Cisco Unity server. See the [“Securing Cisco Unity and the Cisco Unity Server”](#) section on page 8-21.

When you are finished with this chapter, return to the [“Overview of Mandatory Tasks for Installing Cisco Unity”](#) chapter to continue installing the Cisco Unity system.

**Note**

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Determining Whether to Set Up Cisco Unity to Use SSL

When subscribers log on to the Cisco Personal Communications Assistant (PCA), their credentials are sent across the network to Cisco Unity in clear text. The same is true when the Cisco Unity Administrator and the Status Monitor are configured to use the Anonymous authentication method. In addition, the information that subscribers enter on the pages of the Cisco PCA and of the Cisco Unity Administrator (regardless of which authentication method it uses) is not encrypted.

For increased security, we recommend that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol. SSL uses public/private key encryption to provide a secure connection between servers and clients, and uses digital certificates to authenticate servers or servers and clients. (A digital certificate is a file that contains encrypted data that attests to the identity of an organization or entity, such as a computer.)

Using the SSL protocol ensures that all Cisco Unity subscriber credentials—as well as the information that a subscriber enters on any page of the Cisco Unity Administrator and the Cisco PCA—are encrypted as the data is sent across the network. In addition, when you set up Cisco Unity to use SSL, each time that a subscriber tries to access any Cisco Unity web application, the browser will confirm that it is connected with the real Cisco Unity server—and not an entity falsely posing as such—before allowing the subscriber to log on.

To set up a web server such as Cisco Unity to use SSL, you can either obtain a digital certificate from a certificate authority (CA) or use Microsoft Certificate Services available with Windows to issue your own certificate. (A CA is a trusted organization or entity that issues and manages certificates at the request of another organization or entity.) Cost, certificate features, ease of setup and maintenance, and the security policies practiced by the organization are some of the issues to consider when determining whether you should purchase a certificate from a CA or issue your own.

Information on third-party CAs, Microsoft Certificate Services, and SSL is widely available on the Internet, as well as in the Windows and IIS online documentation. Such sources can help you determine whether to use SSL and how to set up a web server to use it.

Installing the Microsoft Certificate Services Component

**Note**

If you do not plan to set up Cisco Unity to use SSL or if you want to use a digital certificate from a certificate authority to set up Cisco Unity to use SSL, skip this section.

Do the procedure in this section if you plan to set up Cisco Unity to use SSL and you want to use the Microsoft Certificate Services available with Windows to issue your own certificate. You may install the component on the Cisco Unity server or on another server.

To Install the Microsoft Certificate Services Component

- Step 1** On the server that will act as your certificate authority (CA) and issue certificates, on the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
- Step 2** Click **Add/Remove Windows Components**.
- Step 3** In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items. When the warning appears about not being able to rename the computer, or to join or be removed from a domain, click **Yes**.
- Step 4** Click **Next**.
- Step 5** Click **Stand-alone Root CA**, and click **Next**. (A stand-alone CA is a CA that does not require Active Directory.)
- Step 6** Follow the on-screen prompts to complete the installation. For information, refer to the Windows documentation.

If a message appears that Internet Information Services is running on the computer and must be stopped before proceeding, click **OK** to stop the services.
- Step 7** In the Completing the Windows Components Wizard dialog box, click **Finish**.
- Step 8** Close the Add Remove Programs dialog box and Control Panel.

Installing and Configuring Cisco Unity Software

To install and configure Cisco Unity software, you use the Cisco Unity Installation and Configuration Assistant to run seven programs in a specific order. The programs:

- Check the system and install the Cisco Unity software.
- Install the Cisco Unity licenses.
- Configure the Cisco Unity services.
- Configure Cisco Unity for the message store.
- Set new default passwords for the Default Administrator and the Default Subscriber templates
- Integrate Cisco Unity with the phone system.
- Configure the Cisco Personal Communications Assistant to use SSL.

Do the following seven subsections in the order listed.

Starting the Cisco Unity Installation and Configuration Assistant and Installing Cisco Unity Software

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Setup program first to install Cisco Unity. The Setup program checks the system, then installs the Cisco Unity software.



Caution

Do not install Cisco Unity remotely by using Windows Terminal Services or other remote-access applications, or the installation may fail.



Caution

Do not install features for which the system is not licensed, or Cisco Unity will shut down.

To Start the Assistant and Install the Cisco Unity Software

Step 1 Log on to Windows by using the Cisco Unity installation account.



Caution

If you have not already done so, disable virus-scanning and Cisco Security Agent services on the server, if applicable. Otherwise, the installation may fail.

Step 2 On Cisco Unity DVD 1 or CD 1, browse to the root directory and double-click **Setup.exe**.

Step 3 If prompted, double-click the language of your choice to continue the installation.

Step 4 On the Cisco Unity Installation and Configuration Assistant Welcome page, click **Continue**.

If the Pre-Installation Requirements page appears, saying that you need to run the Permissions wizard, close the Cisco Unity Installation and Configuration Assistant and see the [“Setting Rights and Permissions with the Cisco Unity Permissions Wizard” section on page 7-4](#). Then log on to Windows by using the Cisco Unity installation account, and return to Step 2.

Step 5 Click **Run the Cisco Unity Setup Program**.

Step 6 If prompted, double-click the language of your choice to continue the installation.

Step 7 On the Welcome page, click **Next**.

Step 8 Enter your name and the company name, and click **Next**.

Step 9 Specify locations for the Cisco Unity application, trace logs, and Unity Messaging Repository (UMR) files. Use the locations you made note of in the [“Determining the Drive Locations for Files on the Cisco Unity Server” section on page 2-4](#).

Step 10 Click **Next**.

Step 11 In the Select Features dialog box:

- a. Check the **Install Cisco Unity** check box.
- b. If the Cisco Unity license includes text to speech, check the **Enable TTS** check box.
If not, uncheck the **Enable TTS** check box.

- c. If the Cisco Unity server or an attached expansion chassis contains Intel Dialogic voice cards, check the **Install Voice Card Software** check box.

If not, uncheck the **Install Voice Card Software** check box.



Note If Windows Server 2003 is installed on the Cisco Unity server, the Install Voice Card Software check box is not available. Circuit-switched phone system integrations that use voice cards are not supported with a Cisco Unity server on which Windows Server 2003 is installed.

Step 12 Click **Next**.

Step 13 Choose the prompt set to install. Use the G.729a system prompt set if voice messages will be recorded and stored in G.729a format. Otherwise, use G.711 (the default).

Note that choosing a system prompt set does not change the default message recording and storage codec. If necessary, you can change the message recording and storage codec later in the installation process.

Step 14 Click **Next**.

Step 15 In the Cisco Unity Languages dialog box, choose the language(s) to install, and click **Next**.

If you installed Windows by using the manufacturer's guided system-setup utility and a retail Windows disc, one of the languages you choose here must match the locale you specified when you installed Windows.



Caution If the locale you specified when you installed Windows does not match any of the installed Cisco Unity languages, Cisco Unity will log errors in the event log and may stop taking calls. The language you choose here must exactly match the locale you selected when you installed Windows. For example, if you chose English (United Kingdom) for locale, you must also choose English (United Kingdom) as one of the Cisco Unity languages. English (Australia) will not work.


If you installed Windows by using the Platform Configuration discs that are shipped with the Cisco Unity server, the locale is automatically set to English (United States). The Cisco Unity Setup program always installs English (United States), so you do not need to choose it as one of the languages to install.

Note that if the system will be using text to speech (TTS) and will be using English (Australia) or English (New Zealand) as the phone language, also install English (United States) or English (United Kingdom) for the TTS language.

Step 16 Set the system-default languages for the phone, graphical user interface (GUI), and TTS, and click **Next**.

Step 17 Follow the on-screen prompts until you are prompted to restart the Cisco Unity server.

- Step 18** The remainder of the procedure depends on whether the server contains Intel Dialogic D/120JCT-Euro or D/240PCI-T1 voice cards:

If the server does not contain Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards	Check the Yes, I Want to Restart My Computer Now check box, and click Finish . Cisco Unity software is now installed.
If the server contains Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards	<p>a. Uncheck the Yes, I Want to Restart My Computer Now check box, and click Finish.</p> <p> Caution If the Cisco Unity server contains Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards, do not restart the server now or you will not be able to access the Cisco Unity Administrator after Cisco Unity is installed.</p> <p>b. Do the procedure under “Software Settings” for your voice card in the “Voice Cards and PIMG Units” appendix.</p> <p>c. Restart the Cisco Unity server.</p>

Installing License Files

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Install License File wizard second to install the Cisco Unity license files.

This section contains two procedures. Do the first procedure on the primary Cisco Unity server and the second procedure on the secondary Cisco Unity server.

To Install the License Files on the Primary Server

- Step 1** Log on to Windows by using the Cisco Unity installation account.
- Step 2** On the Install the Cisco Unity License Files page, click **Run the Cisco Unity Install License File Wizard**.
- Step 3** On the Welcome page, click **Next**.
- Step 4** Click **Add**.
- Step 5** Insert the Cisco Unity license file disk, if applicable.
- (When Cisco Unity was registered on Cisco.com, Cisco replied with an e-mail containing attached file(s) with license(s) for Cisco Unity features. The instructions in the e-mail directed that the attached files be saved. For more information, see the [“Obtaining Cisco Unity License Files”](#) section on page 5-4.)
- Step 6** Browse to drive A or to the location where the license file(s) have been stored.
- Step 7** Double-click the license file to add it to the License Files list.
- If prompted, click **Yes** to copy the license file to the local system.
- Step 8** If you are adding more than one license file, click **Add**, and repeat [Step 6](#) and [Step 7](#) for each license file.

- Step 9** Click **Next**.
- Step 10** In the Licenses dialog box, confirm that the license information is correct.
- Step 11** Click **Next**.
- Step 12** Click **Finish**.

When the wizard is complete, the Configure the Cisco Unity Services page appears in the main window.

To Install the Default License File on the Secondary Server

- Step 1** Log on to Windows by using the Cisco Unity installation account.
- Step 2** On the Install the Cisco Unity License Files page, click **Run the Cisco Unity Install License File Wizard**.
- Step 3** On the Welcome page, click **Next**.
- Step 4** Click **Add**.
- Step 5** Install the default license file:
- Browse to the **CommServer\Licenses** directory.
 - Double-click **CiscoUnity40.lic**.

Click **Next**.

- Step 6** In the Licenses list, confirm that the license information is correct.
- Step 7** Click **Next**.
- Step 8** Click **Finish**.

When the wizard is complete, the Configure the Cisco Unity Services page appears in the main window.

Configuring Services

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Services Configuration wizard third to associate the directory, message store, and local services with accounts you specify.

To Configure Services

- Step 1** On the Configure the Cisco Unity Services page, click **Run the Cisco Unity Services Configuration Wizard**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)
- Step 2** On the Welcome page, click **Next**.
- Step 3** Choose the version of Exchange that is installed on the partner Exchange server that you chose in the [“Determining the Partner Exchange Server”](#) section on page 6-2.

Step 4 Click **Next**.

Step 5 Follow the on-screen prompts to complete the configuration.

When the wizard is complete, the Configure the Cisco Unity Message Store page appears in the main window.

Configuring Cisco Unity for the Message Store

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Message Store Configuration wizard fourth to configure Cisco Unity for the message store.

To Configure Cisco Unity for the Message Store

Step 1 On the Configure the Cisco Unity Message Store page, click **Run the Cisco Unity Message Store Configuration Wizard**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)

Step 2 Confirm that Exchange is running on the partner server that you chose in the “[Determining the Partner Exchange Server](#)” section on page 6-2. If Exchange is not running, configuring the message store on the Cisco Unity server will fail.

Step 3 In the Welcome dialog box, click **Next**.

Step 4 Enter the password for the installation account, and click **Next**.

Step 5 If you did not create a Cisco Unity administration account in the “[Creating the Accounts Required for the Cisco Unity Installation](#)” section on page 7-3, skip to **Step 6**. When installation is complete, you will log on to the Cisco Unity Administrator by using the installation account.

If you created a Cisco Unity administration account in the “[Creating the Accounts Required for the Cisco Unity Installation](#)” section on page 7-3, specify the account:

a. Click **Change**.

b. In the Select User dialog box, double-click the name of the Cisco Unity administration account.

Step 6 Click **Next**.

Step 7 In the Select Partner Message Store dialog box, click **Microsoft Exchange 2000** or **Microsoft Exchange 2003**, depending on the version of Exchange installed on the partner Exchange server, and click **Next**.

Step 8 In the Select Mailbox Location dialog box, choose the partner Exchange server and the mailbox store in which to create new mailboxes, and click **Next**.

Step 9 In the Select Active Directory Containers for New Objects dialog box, choose the domain in which you want Cisco Unity to create users and distribution lists.

If you created custom organizational units for users or distribution lists, click the corresponding **Change** button to specify them here.

Step 10 Click **Next**.

Step 11 Click **OK** to stop Cisco Unity services.

- Step 12** In the Select How Subscribers Will Be Created dialog box, set how administrators will create Cisco Unity subscriber accounts in the Cisco Unity Administrator:

Create New Accounts or Import Existing Accounts	Click if administrators will create subscriber accounts either by adding a new user to Exchange or by importing existing user data from Exchange.
Import Existing Accounts Only	Click if administrators will create subscriber accounts only by importing existing user data from Exchange.

- Step 13** Click **Next**.
- Step 14** By default, the account that you created for Cisco Unity directory services appears. If you want to choose a different account, click **Change**.
- Step 15** Specify a password for the account, and click **Next**.
- Step 16** When message store configuration is complete, click **Finish**.
- When the wizard is complete, the Set New Default Passwords page appears in the main window.

Setting New Default Passwords

From the Cisco Unity Installation and Configuration Assistant, you run the Password Hardening wizard fifth to set new default passwords for the Default Administrator and the Default Subscriber templates.

When all of the following conditions are true, Cisco recommends that you specify an extremely long and complex password for the Active Directory password in the Default Subscriber template:

- Subscribers will access messages only by using the phone.
- Subscribers will not have access to the Cisco Personal Communications Assistant.
- You will be creating Cisco Unity subscribers by using the Cisco Unity Administrator.

When a subscriber is created by using the Cisco Unity Administrator, an Active Directory account is automatically created for that subscriber, too. The password on the Active Directory account is the password in the Default Subscriber template.



Caution

Anyone who knows the password for the Active Directory account, knows the alias for a subscriber, and knows on which Exchange server the voice messages for that subscriber are stored can access those messages.

To Set New Default Passwords

- Step 1** On the Set New Default Passwords page, click **Run the Password Hardening Wizard**.
- Step 2** Follow the on-screen prompts.
- When the Password Hardening wizard finishes, the Integrate the Phone System with Cisco Unity page appears in the main window.

Integrating the Phone System with Cisco Unity

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Telephony Integration Manager (UTIM) sixth to connect Cisco Unity with the phone system.

This section contains two procedures. Do the first procedure on the primary Cisco Unity server and the second procedure on the secondary Cisco Unity server.

To Integrate the Phone System with Cisco Unity on the Primary Server

-
- Step 1** On the Integrate the Phone System with Cisco Unity page, click **Run the Cisco Unity Telephony Integration Manager**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)
 - Step 2** In the right pane of the UTIM, click **Create Integration**.
 - Step 3** Refer to the applicable Cisco Unity integration guide for your phone system to complete the integration. (Cisco Unity integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.)

When the integration is complete, the Set Up the Cisco Personal Communications Assistant to Use SSL page appears in the main window.

To Integrate the Phone System with Cisco Unity on the Secondary Server

-
- Step 1** In the main window of the assistant, click **Run the Cisco Unity Telephony Integration Manager**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)
 - Step 2** In the right pane of the UTIM, click **Create Integration**.
 - Step 3** Fill in the fields with the same values you used for the primary Cisco Unity server, with the exception of the Cisco CallManager Device Name Prefix field value for a Cisco CallManager integration. The value used on the primary Cisco Unity server is different from the value used on the secondary Cisco Unity server. See the applicable Cisco CallManager integration guide.
 - Step 4** When the message appears saying that you have entered more ports than you are allowed, click **OK**. (You will deal with port settings later in the installation.)
 - Step 5** Continue to fill in the fields with the same values you used for the primary Cisco Unity server.

When the integration is complete, the Set Up the Cisco Personal Communications Assistant to Use SSL page appears in the main window.

Setting Up the Cisco Personal Communications Assistant to Use SSL

From the Cisco Unity Installation and Configuration Assistant, you can set up the Cisco PCA to use SSL. Using the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page in the Cisco PCA—are encrypted as the data is sent across the network.

After the Cisco Unity Installation and Configuration Assistant is finished and the Cisco PCA is set up to use SSL, you manually set up the Cisco Unity Administrator and Status Monitor to use SSL. The *Cisco Unity Installation Guide* alerts you when to do the procedure.

If you do not want to set up the Cisco PCA to use SSL, see the “[Skipping Cisco PCA Setup for SSL](#)” section on page 8-11.

To set up the Cisco PCA to use SSL, do the procedures in the applicable section, depending on whether you are using a certificate authority:

- [Setting Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority, page 8-11](#)
- [Setting Up the Cisco PCA to Use SSL by Using a Certificate Authority, page 8-13](#)

If the Cisco Unity server is running Windows Server 2003, you can set up the Cisco Personal Communications Assistant to use SSL now. However, the option to do so by creating a local certificate without a certificate authority has not been automated for Windows Server 2003. If you want to set up the Cisco PCA to use SSL by using this method, you must do so manually. Refer to the “Using SSL to Secure Client/Server Connections” chapter of the *Cisco Unity Security Guide, Release 4.x* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/usg/ex/index.htm.

Skipping Cisco PCA Setup for SSL

Do the procedure in this section if you do not want to set up the Cisco PCA to use SSL. (Note that without SSL when subscribers log on to the Cisco PCA, their credentials will be sent across the network to Cisco Unity in clear text. In addition, the information that subscribers enter on the pages of the Cisco PCA will not be encrypted.)

To Skip Cisco PCA Setup for SSL

-
- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, Click **Do Not Set Up Cisco Personal Communications Assistant to Use SSL**.
- Step 2** Click **Continue**.
- Step 3** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.
-

Setting Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority

To Set Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority

-
- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, click **Create a Local Certificate Without a Certificate Authority**.
- Step 2** Click **Internet Services Manager**.
- Step 3** Expand the name of the Cisco Unity server.
- Step 4** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 5](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 5** Right-click **Default Web Site**, and click **Properties**.

- Step 6** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 7** Under Secure Communications, click **Server Certificate**.
- Step 8** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 9** Click **Create a New Certificate**, and click **Next**.
- Step 10** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
- Step 11** Enter a name and a bit length for the certificate.
We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.
- Step 12** Click **Next**.
- Step 13** Enter the organization information, and click **Next**.
- Step 14** For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.



Caution The name must exactly match the host portion of any URL that will access the system by using a secure connection.

- Step 15** Click **Next**.
- Step 16** Enter the geographical information, and click **Next**.
- Step 17** Specify the certificate request file name and location, and write down the file name and location because you will need the information later in this procedure.
- Step 18** Click **Next**.
- Step 19** Verify the request file information, and click **Next**.
- Step 20** Click **Finish** to exit the Web Server Certificate wizard.
- Step 21** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 22** Close the Internet Services Manager window.
- Step 23** In the Cisco Unity Installation and Configuration Assistant, in the Enter Certificate Request File box, enter the full path and file name of the certificate request file that you specified in [Step 17](#).
- Step 24** Click **Create Certificate**.
- Step 25** Click **Internet Services Manager**.
- Step 26** Expand the name of the Cisco Unity server.
- Step 27** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 28](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 28** Right-click **Default Web Site**, and click **Properties**.
- Step 29** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 30** Under Secure Communications, click **Server Certificate**.
- Step 31** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 32** Click **Process the Pending Request and Install the Certificate**.
- Step 33** Click **OK**.
- Step 34** In the Process a Pending Request dialog box, click **OK** to accept the default path and file name of the pending certificate request.

- Step 35** In the Certificate Summary dialog box, click **Next**.
 - Step 36** Click **Finish** to exit the Web Server Certificate wizard.
 - Step 37** Click **OK** to Close the Default Web Site Properties dialog box.
 - Step 38** Close the Internet Services Manager window.
 - Step 39** In the Cisco Unity Installation and Configuration Assistant, click **Enable Cisco PCA to Use SSL**.
 - Step 40** Click **Internet Services Manager**.
 - Step 41** Right-click the name of the Cisco Unity server, and click **Restart IIS**.
 - Step 42** In the Stop/Start/Restart dialog box, click **Restart Internet Services on <Servername>**.
 - Step 43** Click **OK**.
 - Step 44** Close the Internet Services Manager window.
 - Step 45** In the Cisco Unity Installation and Configuration Assistant, click **Continue**.
 - Step 46** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.
-

Setting Up the Cisco PCA to Use SSL by Using a Certificate Authority

This section contains four procedures.

If you are using Microsoft Certificate Services to issue your own certificate, do all four procedures in the order listed.

If you are using a certificate purchased from a certificate authority (for example, VeriSign), do only the fourth procedure, “[To Install the Certificate](#).”

To Create a Certificate Request by Using Microsoft Certificate Services

- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, click **Use a Certificate Authority**.
- Step 2** Click **Internet Services Manager**.
- Step 3** Expand the name of the Cisco Unity server.
- Step 4** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 5](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 5** Right-click **Default Web Site**, and click **Properties**.
- Step 6** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 7** Under Secure Communications, click **Server Certificate**.
- Step 8** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 9** Click **Create a New Certificate**, and click **Next**.
- Step 10** Click **Prepare the Request Now, But Send It Later**, and click **Next**.

Step 11 Enter a name and a bit length for the certificate.

We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.

Step 12 Click **Next**.

Step 13 Enter the organization information, and click **Next**.

Step 14 For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.



Caution The name must exactly match the host portion of any URL that will access the system by using a secure connection.

Step 15 Click **Next**.

Step 16 Enter the geographical information, and click **Next**.

Step 17 Specify the certificate request file name and location, and write down the file name and location because you will need the information in the next procedure.

Save the file to a disk or to a directory that the certificate authority (CA) server can access.

Step 18 Click **Next**.

Step 19 Verify the request file information, and click **Next**.

Step 20 Click **Finish** to exit the Web Server Certificate wizard.

Step 21 Click **OK** to Close the Default Web Site Properties dialog box.

Step 22 Close the Internet Services Manager window.

Step 23 Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.

To Submit the Certificate Request by Using Microsoft Certificate Services

Step 1 On the server that is acting as the CA, on the Windows Start menu, click **Run**.

Step 2 Run **Certreq**.

Step 3 Browse to the directory where you saved the certificate request file, and double-click the file.

Step 4 Click the CA to use, and click **OK**.

Once the CA submits the certificate request, it assigns a pending status by default for added security. This requires a person to verify the authenticity of the request and to manually issue the certificate.

To Issue the Certificate by Using Microsoft Certificate Services

Step 1 On the server that is acting as the CA, on the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.

Step 2 In the left pane of the Certification Authority window, expand **Certification Authority**.

- Step 3** Expand <Certification Authority name>.
 - Step 4** Click **Pending Requests**.
 - Step 5** In the right pane, right-click the request, and click **All Tasks > Issue**.
 - Step 6** In the left pane, click **Issued Certificates**.
 - Step 7** In the right pane, double-click the certificate to open it.
 - Step 8** Click the **Details** tab.
 - Step 9** In the Show list, choose <All>, and click **Copy to File**.
 - Step 10** On the Certificate Export wizard Welcome page, click **Next**.
 - Step 11** Accept the default export file format **DER encoded binary X.509 (.CER)**, and click **Next**.
 - Step 12** Specify a file name and a location that the Cisco Unity server can access, and click **Next**.
 - Step 13** Verify the settings, and click **Finish**.
 - Step 14** Click **OK** to close the Certificate Details dialog box.
 - Step 15** Close the Certification Authority window.
-

To Install the Certificate

- Step 1** On the Cisco Unity server, double-click the **CUICA** icon on the desktop.
- Step 2** In the Cisco Unity Installation and Configuration Assistant, click **Use a Certificate Authority**.
- Step 3** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, at Step 3, click **Internet Services Manager**.
- Step 4** Expand the name of the Cisco Unity server.
- Step 5** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 6](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 6** Right-click **Default Web Site**, and click **Properties**.
- Step 7** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 8** Under Secure Communications, click **Server Certificate**.
- Step 9** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 10** Click **Process the Pending Request and Install the Certificate**, and click **Next**.
- Step 11** Browse to the directory of the certificate (.cer) file, and double-click the file.
- Step 12** Verify the certificate information, and click **Next**.
- Step 13** Click **Finish** to exit the Web Server Certificate wizard.
- Step 14** Click **OK** to close the Default Web Site Properties dialog box.
- Step 15** Close the Internet Services Manager window.
- Step 16** In the Cisco Unity Installation and Configuration Assistant, click **Enable Cisco PCA to Use SSL**.
- Step 17** Restart IIS:
 - a. Click **Internet Services Manager**.

- b. Right-click the name of the Cisco Unity server, and click **Restart IIS**.
- c. In the Stop/Start/Restart dialog box, click **Restart Internet Services on <Servername>**.
- d. Click **OK**.
- e. Close the Internet Services Manager window.

Step 18 Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.

Installing the Cisco Unity Service Release, If Available

The service release—a rollup of Cisco Unity engineering specials—is released about three months after an initial release. To determine whether the service release is available for your version of Cisco Unity and, if so, to get download and installation instructions, refer to *Release Notes for Cisco Unity <Version> Service Release 1* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Testing the Phone System Integration

Test the integration with the phone system. Refer to the Cisco Unity integration guide for your phone system.

Test only the integration with the primary Cisco Unity server now. You test the integration with the secondary Cisco Unity server after you set up failover. The *Cisco Unity Failover Configuration and Administration Guide* instructs you when and how to test the secondary server.

Note that you use the Cisco Unity Administrator for part of the integration test. Use the user name and password for the account that you selected to administer Cisco Unity.

Excluding from Virus Scanning the Directory in Which Cisco Unity Is Installed



Note

If virus-scanning software is not installed on the Cisco Unity server, skip this section.

You exclude from scanning the directory in which Cisco Unity is installed, as well as all subdirectories, so that the Cisco Unity Administrator and the Cisco Unity Assistant will work properly.

To Exclude from Virus Scanning the Directory in Which Cisco Unity Is Installed

- Step 1** Refer to the virus-scanning software Help for instructions on excluding directories from scanning.
 - Step 2** Exclude from virus scanning the directory in which Cisco Unity is installed (the default directory is CommServer) and all subdirectories under the directory.
-

Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL

**Note**

If you are not setting up Cisco Unity to use SSL, skip this section.

Using the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page in the Cisco Unity Administrator—are encrypted as the data is sent across the network.

To Set Up the Cisco Unity Administrator and Status Monitor to Use SSL

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** Expand the name of the Cisco Unity server.
- Step 3** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 4](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 4** Expand **Default Web Site**.
- Step 5** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 6** In the Properties dialog box, set the Web directory to use SSL:
 - a. Click the **Directory Security** tab.
 - b. Under Secure Communications, click **Edit**.
 - c. Check the **Require Secure Channel (SSL)** check box.
 - d. Click **OK** to close the Secure Communications dialog box.
 - e. Click **OK** to close the Properties dialog box.
- Step 7** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
- Step 8** Repeat [Step 6](#) to set the SAWeb directory to use SSL.
- Step 9** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 10** Repeat [Step 6](#) to set the Status directory to use SSL.
- Step 11** Under Default Web Site, double-click **AvXml**.
- Step 12** In the right pane, right-click **AvXml.dll**, and click **Properties**.
- Step 13** In the Properties dialog box, click the **File Security** tab.
- Step 14** Under Secure Communications, click **Edit**.
- Step 15** Check the **Require Secure Channel (SSL)** check box.
- Step 16** Click **OK** to close the Secure Communications dialog box.
- Step 17** Click **OK** to close the AvXml.dll Properties dialog box.
- Step 18** Close the Internet Services Manager window.

Securing the Example Administrator Account Against Toll Fraud

It is possible for a malicious user to dial into Cisco Unity, log on as the Example Administrator by using the default extension and password, and configure Cisco Unity to forward calls to phone numbers for which there are charges or to reconfigure greetings so an operator believes the messaging system is personally accepting collect-call charges. To help secure Cisco Unity against toll fraud, we strongly recommend that you change the phone password for the Example Administrator account after Cisco Unity is installed.

To Change the Password on the Example Administrator Account

-
- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page.
- Step 2** Click the **Find** icon.
- Step 3** On the Find and Select Subscriber page, click **Find**.
- Step 4** Click **Example Administrator**.
- Step 5** In the left pane, click **Phone Password**.
- Step 6** In the right pane, check the **User Cannot Change Password** check box.
- Step 7** Check the **Password Never Expires** check box.
- Step 8** Under **Reset Phone Password**, enter and confirm a new password by using digits 0 through 9.

We recommend that you enter a long and nontrivial password; 20 digits or more is desirable. (The minimum length of the password is set on the Subscribers > Account Policy > Phone Password Restrictions page.) In a nontrivial password:

- The digits are not all the same (for example, 9999).
- The digits are not consecutive (for example, 1234).
- The password is not the same as the extension assigned to the example account.
- The password does not spell the name of the example account, the name of the company, the name of the IT manager, or any other obvious words.

- Step 9** Click the **Save** icon.
- Step 10** Close the Cisco Unity Administrator.
-

Moving the Data Store Databases and Transaction Logs

The Cisco Unity data store includes several databases and their corresponding transaction logs. Because the Cisco Unity and Reports databases and their transaction logs are the fastest-growing data store files, you place them on the system in a location that makes optimum use of system storage capacity.

As you do the procedure in this section, if applicable, refer to the drive locations you made note of in the [“Determining the Drive Locations for Files on the Cisco Unity Server”](#) section on page 2-4.

For more information on moving SQL Server databases and transaction logs, refer to Microsoft documentation.

To Move the SQL Server Databases and Transaction Logs

- Step 1** Stop Cisco Unity. (Right-click the **Cisco Unity** icon in the system tray, then click **Stop Cisco Unity**; if the Cisco Unity icon is not available, browse to the **CommServer** directory and double-click **AvCsTrayStatus.exe**.)
- Step 2** In Task Manager, end the Cisco Unity tray icon process:
- Right-click in an empty space on the taskbar and click **Task Manager**.
 - Click the **Processes** tab.
 - Click the **Image Name** column twice to sort by process name.
 - Click **AvCsTrayStatus**.
 - Click **End Process**.
 - Click **Yes** to confirm.
 - Close **Task Manager**.
- Step 3** Stop the AvCsGateway service:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - In the right pane, right-click **AvCsGateway**, and click **Stop**.
 - Close the Services MMC.
- Step 4** Detach the ReportDB and UnityDb databases:
- On the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**.
 - In the left pane, expand **Microsoft SQL Servers > SQL Server Group > (local) (Windows NT) > Databases**.
 - Right-click **ReportDb**, and click **All Tasks > Detach Database**.
 - If the OK button is unavailable, click **Clear**, and click **OK** to confirm that you want to clear connections.
 - Click **OK** to detach the ReportDB database.
 - Click **OK** to confirm.
 - Repeat Step **c.** through Step **f.** to detach the UnityDb database.
- Step 5** Close SQL Server Enterprise Manager.
- Step 6** In Windows Explorer, create the new directories for Cisco Unity data and for transaction logs on the drive locations you made note of in the [“Determining the Drive Locations for Files on the Cisco Unity Server”](#) section on page 2-4. Use directory names that are easy to remember, for example:

UnityDb.mdf and ReportDb.mdf	<Database destination drive>\<Path>\UnityData
ReportDb_log.ldf and UnityDb_log.ldf	<Log file destination drive>\<Path>\UnityLogs

- Step 7** In Windows Explorer, move UnityDb.mdf and ReportDb.mdf from Program Files\Microsoft SQL Server\MSSQL\Data to the new directory for Cisco Unity databases.
- Step 8** In Windows Explorer, move ReportDb_log.ldf and UnityDb_log.ldf from Program Files\Microsoft SQL Server\MSSQL\Data to the new directory for Cisco Unity transaction logs.

Step 9 Using OSQL, reattach the databases:



Caution If you put the databases and the transaction log in separate locations, as recommended for most systems, you must use OSQL to reattach the databases because SQL Server Enterprise Manager does not support attaching a database when the corresponding log file is not in the same directory.

- a. On the Windows Start menu, click **Run**.
- b. Run **cmd**.
- c. Start OSQL by entering **OSQL -E** on the command line.



Caution Use **-E**, not **-e**.

- d. Enter **use master** and press **Enter**.
- e. Enter **go** and press **Enter**.
- f. Enter **EXEC sp_attach_db 'UnityDb', '<Database destination drive>\<New database directory path>UnityDb.mdf', '<Log file destination drive>\<New log file directory path>UnityDb_log.ldf'** and press **Enter**.
- g. Enter **go** and press **Enter**.
If you specified an invalid path or file name, an error message appears in the command window. Re-run Step **f**. and Step **g**. with the correct information.
- h. Enter **EXEC sp_attach_db 'ReportDb', '<Database destination drive>\<New database directory path>ReportDb.mdf', '<Log file destination drive>\<New log file directory path>ReportDb_log.ldf'** and press **Enter**.
- i. Enter **go** and press **Enter**.
If you specified an invalid path or file name, an error message appears in the command window. Re-run Step **h**. and Step **i**. with the correct information.

Step 10 Enter **exit** and press **Enter** to close OSQL.

Step 11 On the Windows Start menu, click **Programs > Startup > AvCsTrayStatus** to restart the Cisco Unity tray icon.

- Step 12** When the tray icon appears in the Windows taskbar, use it to restart Cisco Unity.
-

Re-enabling Virus-Scanning and Cisco Security Agent Services



Note If virus-scanning software or Cisco Security Agent for Cisco Unity is not installed on the Cisco Unity server, skip this section.

You re-enable virus-scanning and Cisco Security Agent services now that all of the software installations that could have been affected if the services were running are complete.

To Re-enable and Start Virus-Scanning and Cisco Security Agent Services

- Step 1** Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 3** Re-enable and start each virus-scanning service and the Cisco Security Agent service:
- In the right pane, double-click the service.
 - On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
 - Click **Start** to start the service.
 - Click **OK** to close the Properties dialog box.
- Step 4** When the services have been re-enabled, close the Services MMC.
-

Securing Cisco Unity and the Cisco Unity Server

We strongly recommend that you secure Cisco Unity and the Cisco Unity server. Refer to the *Cisco Unity Security Guide* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/usg/ex/index.htm.



Installing Optional Software

In this chapter, you do the following tasks in the order listed:

1. Install RSA SecurID, if applicable. See the “[Installing RSA SecurID](#)” section on page 9-1.
2. Install Symantec pcAnywhere, if applicable. See the “[Installing Symantec pcAnywhere](#)” section on page 9-1.
3. Install other optional software, if applicable. See the “[Installing Other Optional Software](#)” section on page 9-3.



Caution

Do not install Outlook on the Cisco Unity server, or Cisco Unity may not notify subscribers of new messages.

When you are finished with this chapter, return to the “[Overview of Mandatory Tasks for Installing Cisco Unity](#)” chapter to continue installing the Cisco Unity system.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Installing RSA SecurID

For supported versions of RSA SecurID, refer to *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm.

Follow the manufacturer instructions to install RSA SecurID.

The “[Overview of Mandatory Tasks for Installing Cisco Unity](#)” chapter alerts you when to configure RSA SecurID later in the installation process.

Installing Symantec pcAnywhere

For supported versions of Symantec pcAnywhere, refer to *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm.

Follow the manufacturer instructions to install pcAnywhere. See also the “[Recommended Configuration for pcAnywhere](#)” section, below.

The remote-access software can be installed on the Cisco Unity server in addition to Windows Terminal Services (which is the default remote-access software for the Cisco Unity server and is included with Windows 2000). Use an external modem with pcAnywhere.

Recommended Configuration for pcAnywhere

We recommend that you do the following three procedures in the order listed to configure pcAnywhere to avoid video problems, screen-refresh problems, and a possible problem with the server not responding after pcAnywhere disconnects.

To Configure pcAnywhere So That It Does Not Start Automatically When You Restart the Server

-
- Step 1** On the Windows Start menu, click **Programs > Symantec pcAnywhere**.
 - Step 2** In the pcAnywhere toolbar, click **Hosts**.
 - Step 3** Right-click the **Modem** icon or the host that is configured for a modem, and click **Properties**.
 - Step 4** In the pcAnywhere Host Properties dialog box, click the **Settings** tab.
 - Step 5** In the Host Startup section, uncheck the **Launch with Windows** check box.
 - Step 6** Click **OK** to close the pcAnywhere Host Properties dialog box.
-

To avoid a pcAnywhere video problem, we recommend that you change the pcAnywhere video mode. (The problem is described in Symantec Knowledge Base article 2001040615242112.)

To Change the pcAnywhere Video Mode to Compatibility

-
- Step 1** In pcAnywhere, on the pcAnywhere Tools menu, click **Options**.
 - Step 2** On the Host Operation tab, under Video Mode Selection, click **Compatibility**.
 - Step 3** Click **OK**.
 - Step 4** Exit pcAnywhere.
-

To avoid a pcAnywhere problem with slow or partial screen refreshes on multiprocessor host computers, and a possible problem in which the host computer stops responding when pcAnywhere disconnects, we recommend that you add a registry entry that sets pcAnywhere to run on one or more specific processors. (The problem is described in Symantec Knowledge Base article 199861984643.)

Be aware that setting pcAnywhere to run on a specific processor may affect performance on the Cisco Unity server if someone uses pcAnywhere to access the server during peak hours.

To Set pcAnywhere to Run on One or More Specific Processors

Step 1 Start Regedit.



Caution Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (Refer to the “Restoring” topics in Registry Editor Help.) Note that registry changes on one server in a Cisco Unity failover pair must be made manually on the other server, because registry changes are not replicated. If you have any questions about changing registry key settings, contact Cisco TAC.

Step 2 If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 3 Expand the key
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Host

Step 4 Add a DWORD value named **ProcessorMask**, and set the value depending on which processor you want to use (for example, to make pcAnywhere run on the second processor only, set ProcessorMask to 2):

0	All processors
1	First processor
2	Second processor
4	Third processor
8	Fourth processor

To allow pcAnywhere to run on more than one processor, set the value of ProcessorMask to the sum of the corresponding values. (For example, to make pcAnywhere run on the third and fourth processors, set ProcessorMask to 12 [4 + 8].)

Step 5 Either stop and restart the pcAnywhere host service, or restart the Cisco Unity server.

Installing Other Optional Software

For information on supported software, refer to *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm.

Follow the manufacturer instructions to install other optional software.



Caution Do not install Outlook on the Cisco Unity server, or Cisco Unity may not notify subscribers of new messages.



Setting Up Authentication for the Cisco Unity Administrator

In this chapter, you do the following tasks in the order listed:



Note

If you are installing the secondary Cisco Unity server now, skip Task 1.

1. Determine the authentication method that you want to use for the Cisco Unity Administrator. See the [“Determining the Authentication Method to Use for the Cisco Unity Administrator”](#) section on page 10-1.
2. Configure IIS so that the Cisco Unity Administrator and Status Monitor use the Anonymous authentication method, if applicable. See the [“Configuring IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication”](#) section on page 10-5.

When you are finished with this chapter, return to the [“Overview of Mandatory Tasks for Installing Cisco Unity”](#) chapter to continue installing the Cisco Unity system.



Note

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Determining the Authentication Method to Use for the Cisco Unity Administrator

The Cisco Unity Administrator is the website used to do most administration tasks, including: determining system schedules, specifying settings for individual subscribers (or for a group of subscribers by using a subscriber template), and implementing a call management plan.

To access the Cisco Unity Administrator, Cisco Unity requires that the identity of the administrator is authenticated by a name and password. You can choose which IIS authentication method that you want to use for the Cisco Unity Administrator. (Note that the authentication method you choose also applies to the Cisco Unity Status Monitor.)



Note

Until a Cisco Unity subscriber account is created for the purpose of administering Cisco Unity, you must use the Windows credentials associated with the administration account that was selected when Cisco Unity was installed to log on to the Cisco Unity Administrator.

The following three subsections discuss the available authentication methods and how they work:

- [Authentication Methods Available for the Cisco Unity Administrator, page 10-2](#)
- [How Integrated Windows Authentication Works with the Cisco Unity Administrator, page 10-3](#)
- [How Anonymous Authentication Works with the Cisco Unity Administrator, page 10-4](#)

Authentication Methods Available for the Cisco Unity Administrator

By default, IIS is configured so that the Cisco Unity Administrator uses the Integrated Windows authentication method (formerly called NTLM or Windows NT Challenge/Response authentication) to authenticate the user name and password. If you prefer, you can configure IIS so that the Cisco Unity Administrator uses the Anonymous authentication method instead.

To determine which authentication method to use, first discuss it with the network administrator to confirm that the method you choose aligns with the existing authentication scheme in the organization and addresses security concerns for the site. In addition, consider the advantages and disadvantages of using each authentication method with the Cisco Unity Administrator, as shown in [Table 10-1](#) and [Table 10-2](#).

Refer to the Microsoft website for general information on the strengths and weaknesses of using either Integrated Windows or Anonymous authentication.

[Table 10-1](#) lists the advantages and disadvantages of using Integrated Windows authentication with the Cisco Unity Administrator.

Table 10-1 Using Integrated Windows Authentication with the Cisco Unity Administrator

Advantages	Disadvantages
<ul style="list-style-type: none"> • User credentials are not sent across the network. Instead, Internet Explorer and Windows use a challenge/response mechanism to authenticate the user. • By default, IIS is already set up so that the Cisco Unity Administrator uses the Integrated Windows authentication method. 	<ul style="list-style-type: none"> • Windows cannot validate the identity of a user when the user is logged on to an untrusted domain. To solve this problem, configure each subscriber browser to prompt for a user name and password so that subscribers can enter the applicable credentials for the domain that the Cisco Unity server is in. Alternatively, you can establish trusts across domains. • When subscribers log on to the Cisco Unity Administrator from another domain, they are prompted to re-enter their credentials each time that they want to use the phone as a recording and playback device for the Media Master.

Table 10-2 lists the advantages and disadvantages of using Anonymous authentication with the Cisco Unity Administrator.

Table 10-2 Using Anonymous Authentication with the Cisco Unity Administrator

Advantages	Disadvantages
<ul style="list-style-type: none"> When subscribers log on to the Cisco Unity Administrator from another domain, they can enter the applicable credentials on the Cisco Unity Log On page for the domain that the Cisco Unity server is in. Thus, you do not need to configure each subscriber browser to prompt for a user name and password, nor do you need to establish trusts across domains. When subscribers log on to the Cisco Unity Administrator from another domain, they are not prompted to re-enter their credentials each time that they want to use the phone as a recording and playback device for the Media Master. 	<ul style="list-style-type: none"> When a subscriber enters Windows domain account credentials on the Cisco Unity Log On page, the credentials are sent across the network in clear text. To solve this problem, set up Cisco Unity to use SSL. By default, IIS is not set up so that the Cisco Unity Administrator uses the Anonymous authentication method. You must configure it.

How Integrated Windows Authentication Works with the Cisco Unity Administrator

When IIS is configured so that the Cisco Unity Administrator uses Integrated Windows authentication, Cisco Unity does not authenticate the subscriber. Instead, the identity of the user is verified by Windows.

- A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
- Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
- IIS indicates that it cannot authenticate the user.
- When Internet Explorer is configured to prompt for a user name and password, it displays a dialog box and waits for the subscriber to enter the Windows domain account credentials. Once the subscriber enters the credentials, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it sends IIS an encrypted message regarding the Windows domain account based on the credentials that the subscriber entered in the dialog box.

When Internet Explorer is not configured to prompt for a user name and password, Internet Explorer tries to get the Cisco Unity Administrator web page again, but this time, it sends IIS an encrypted message regarding the Windows domain account based on the credentials that the subscriber entered to log on to Windows.

In both scenarios, the user password—or any representation of the password—is not sent across the network because authentication relies on Windows challenge/response.

- If Windows can confirm the identity of the Windows domain user, then IIS sends the user and domain name to Cisco Unity, and the process continues with Step 6.

If Windows cannot validate the identity of the Windows domain user (as would be the case if the subscriber logged on to an untrusted domain), Internet Explorer prompts the subscriber for a user name and password. Once again, the credentials are not sent across the network; instead, Internet Explorer sends IIS an encrypted message regarding the Windows domain account based on the credentials that were entered in the dialog box. If Windows still cannot authenticate the user, Internet Explorer displays a message indicating that access to the website is denied because the domain account is unknown.

6. Cisco Unity checks to see that there is a subscriber account associated with the Windows domain account used to authenticate the subscriber and that the subscriber account has COS rights to access the Cisco Unity Administrator.
7. If a subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page that indicates that the subscriber does not have permission to view the Cisco Unity Administrator website.

How Anonymous Authentication Works with the Cisco Unity Administrator

When IIS is configured so that the Cisco Unity Administrator uses Anonymous authentication, Cisco Unity authenticates the credentials that subscribers enter on the Cisco Unity Log On page.

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco Unity Administrator website.
2. Internet Explorer tries to get the home page for the Cisco Unity Administrator from IIS.
3. IIS allows access to Cisco Unity based on the privileges for the IUSR_[computer name] account. (This is the anonymous account that IIS uses for Anonymous authentication by default.)
4. Cisco Unity presents the Cisco Unity Log On page, which is displayed in the browser.
5. The Log On page prompts subscribers to enter their Windows domain account credentials, as shown in [Table 10-3](#).

Table 10-3 Cisco Unity Log On Page for Windows Credentials

Field Name	Description
User Name	Subscribers must enter the alias for the Windows domain account that is associated with their Cisco Unity subscriber account. (For example, they can enter tcampbell or they can enter the full path, tcampbell@<domain name>.) If subscribers enter the full path for their alias, they do not need to complete the Domain field.
Password	Subscribers must enter the password for their Windows domain account.
Domain	Subscribers must enter the name of the domain in which their Windows domain account resides, unless they entered a full path for their alias in the User Name field. If that is the case, subscribers can leave the field blank.

6. Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To solve this security problem, set up Cisco Unity to use SSL.)
7. Cisco Unity requests authentication of the credentials from Windows.
8. If Cisco Unity can authenticate the Windows credentials, Cisco Unity then confirms that there is a subscriber account associated with the Windows domain account used to authenticate the subscriber and that the subscriber account has COS rights to access the Cisco Unity Administrator. The process continues with Step 9.

If the credentials cannot be authenticated, Cisco Unity presents a web page that indicates that the subscriber does not have permission to view the Cisco Unity Administrator website.

9. If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco Unity Administrator website, which is displayed in the browser.

If the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page, which indicates that the subscriber does not have permission to view the Cisco Unity Administrator website.

Configuring IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication

**Note**

If you decided that the Cisco Unity Administrator will use the Integrated Windows authentication method, skip this section.

This section contains two procedures. Do the applicable procedure, depending on whether the Cisco Unity server is running Windows Server 2003 or Windows 2000 Server.

To Configure IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication (Windows Server 2003)

- Step 1** On the Windows Start menu, click **Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** In the left pane, right-click **Application Pools**, and click **Properties**.
- Step 3** In the Application Pools Properties dialog box, click the **Identity** tab.
- Step 4** In the Predefined list, click **Local System**.
- Step 5** Click **OK** to close the Application Pools Properties dialog box.
- Step 6** In the IIS Manager message box, click **Yes** to confirm that you want to run this application pool as Local System.
- Step 7** In the left pane of Internet Information Services (IIS) Manager, expand **Web Sites > Default Web Site**.
- Step 8** Right-click **SAWeb**, and click **Properties**.
- Step 9** In the SaWeb Properties dialog box, click the **Directory Security** tab.
- Step 10** In the Authentication and Access Control section, click **Edit**.
- Step 11** In the Authentication Methods dialog box, check the **Enable Anonymous Access** check box.
- Step 12** Uncheck the **Integrated Windows Authentication** check box.
- Step 13** Click **OK** to close the Authentication Methods dialog box.
- Step 14** Click **OK** to close the SaWeb Properties dialog box.
- Step 15** Repeat [Step 8](#) through [Step 14](#) for the following virtual directories:
 - Status
 - StatusXml

- Web
-

To Configure IIS So That the Cisco Unity Administrator and Status Monitor Use Anonymous Authentication (Windows 2000 Server)

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** In the Internet Information Services window, double-click <System-name> to expand it.
- Step 3** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 4** In the Properties dialog box, set the authentication method for the Web directory:
- Click the **Directory Security** tab.
 - Under Anonymous Access and Authentication Control, click **Edit**.
 - In the Authentication Methods dialog box, check the **Anonymous Access** check box.
 - Uncheck the **Integrated Windows Authentication** check box.
 - Click **OK** to close the Authentication Methods dialog box.
 - Click **OK** to close the Properties dialog box.
- Step 5** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
- Step 6** Repeat [Step 4](#) to set the authentication method for the SAWeb directory.
- Step 7** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 8** Repeat [Step 4](#) to set the authentication method for the Status directory.
- Step 9** Under Default Web Site, click **AvXML**.
- Step 10** In the AvXML directory, right-click **AvXML.dll**, and click **Properties**.
- Step 11** Repeat [Step 4](#) to set the authentication method for AvXML.dll.
- Step 12** Close the Internet Information Services window.
-



Voice Cards and PIMG Units

This appendix contains the following sections:

- [Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro, page A-1](#)
- [Intel Dialogic D/120JCT-LS and D/120JCT-Euro, page A-4](#)
- [Intel Dialogic D/240PCI-T1, page A-8](#)
- [Intel NetStructure PBX-IP Media Gateway \(PIMG\), page A-11](#)
- [Removing Intel Dialogic Voice Card Software, page A-12](#)

Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro

The D/41EPCI, D/41JCT-LS, and D/41JCT-Euro voice cards provide four independent voice-processing ports in a single PCI slot. The cards connect four phone-line interface circuits directly to analog loop-start lines by using RJ-11 connectors.

If you are installing cards that have H.100 connectors, you need an H.100 cable that has at least as many connectors as you have cards (you must connect all cards by using a single cable) but no more than five extra connectors.

Figure A-1 D/41EPCI Top and Side Views

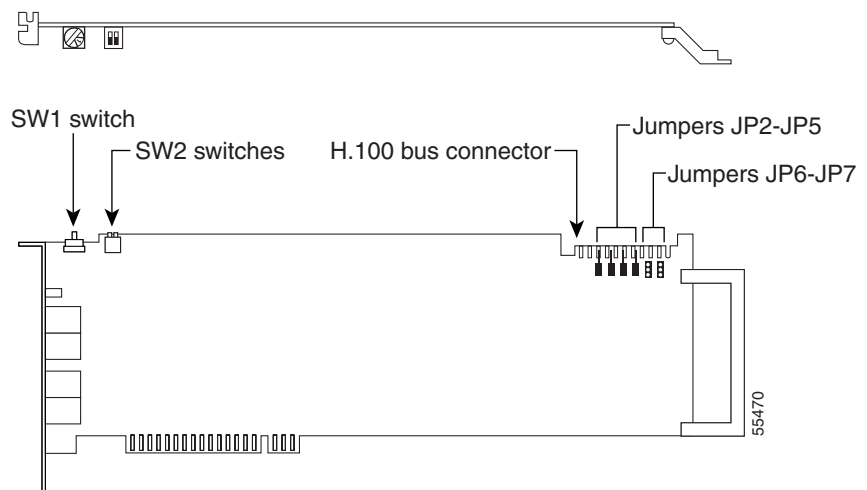


Figure A-2 D/41JCT-LS, and D/41JCT-Euro Top and Side Views

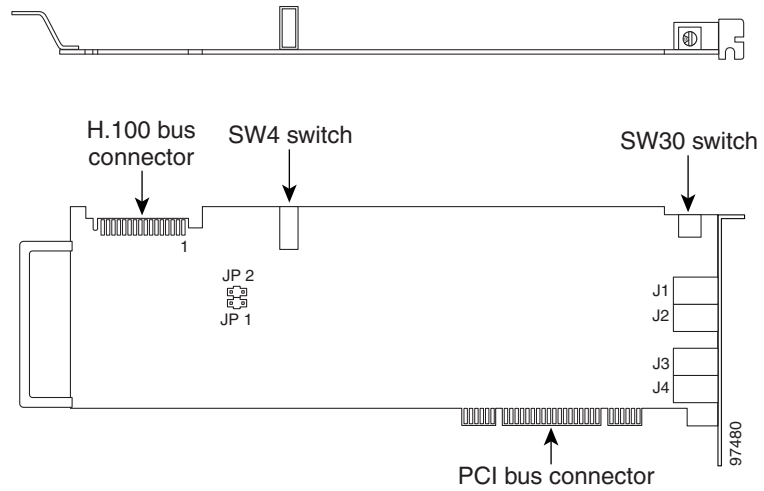
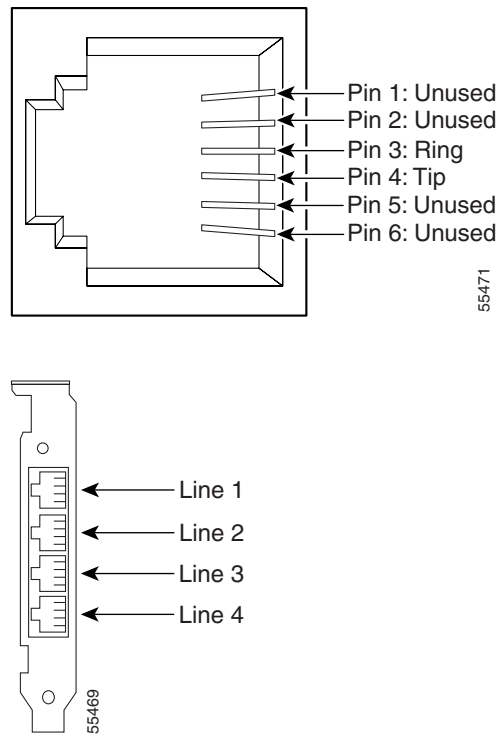


Figure A-3 D/41EPCI, D/41JCT-LS, and D/41JCT-Euro Connection Pinouts and Backplate

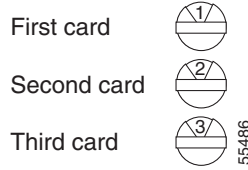


Hardware Settings

To Set the D/41EPCI Card Switches and Jumpers

- Step 1** Set the rotary switch (SW1) to a unique value for each card.

Each Intel Dialogic card in the Cisco Unity server or expansion chassis must have a unique value, starting with **1** and continuing in sequence on subsequent cards. For example, set the rotary switch on the first three voice cards as shown below. This is also the order in which you install the cards in the server or expansion chassis.



Step 2 Set SW2 switches to **Off** on each card.

Step 3 Settings for jumpers JP2 through JP5 depend on the number of D/41EPCI voice cards in the Cisco Unity server or expansion chassis:

One card	Set jumpers JP2 through JP5 to Off (Figure A-4) on the card.
Two cards	Set jumpers JP2 through JP5 to On (Figure A-5) on both cards.
Three or more cards	Set jumpers JP2 through JP5 to On (Figure A-5) on the first and last cards. Set jumpers JP2 through JP5 to Off (Figure A-4) on all other cards.

Figure A-4 D/41EPCI Jumpers JP2 Through JP 5: Off

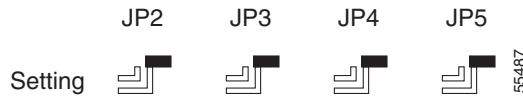
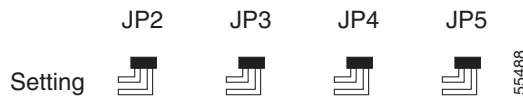
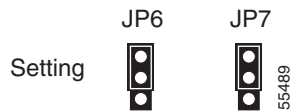


Figure A-5 D/41EPCI Jumpers JP2 Through JP 5: On



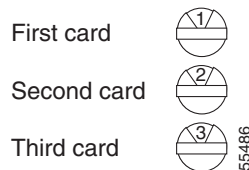
Step 4 On jumpers JP6 and JP7, install shunts on the top two pins (1 and 2).



To Set the D/41JCT-LS and D/41JCT-Euro Card Switches and Jumpers

Step 1 Set the rotary switch (SW30) to a unique value for each card.

Each Intel Dialogic card in the Cisco Unity server or expansion chassis must have a unique value, starting with **1** and continuing in sequence on subsequent cards. For example, set the rotary switch on the first three voice cards as shown below. This is also the order in which you install the cards in the Cisco Unity server or expansion chassis.



Step 2 Set the SW4 hook-state switch to **Off**.

Step 3 Settings for jumpers JP1 and JP2 are as follows:

Jumper JP1 is reserved. Do not install a shunt across the pins of JP1.

Set jumper JP2 according to the number of D/41JCT-LS or D/41JCT-EURO cards in the server or expansion chassis:

One card	Unterminated (the default configuration).
Two or more cards	Install the shunt on the JP2 jumper of a card to terminate the CT bus (H.100 signal) at that card. Terminate only the first and last cards on the CT bus cable.

Intel Dialogic D/120JCT-LS and D/120JCT-Euro

The D/120JCT-LS and D/120JCT-Euro voice cards each provide 12 channels of call-processing and loop-start interfaces in a single PCI slot. The D/120JCT-LS is used in North America, South America, and Japan, and the D/120JCT-Euro is used in Europe, Australia, and New Zealand. The cards connect 12 analog loop-start phone lines to 12 onboard call-processing resources by using RJ-14 connectors.

We recommend using the newer Revision 2 Universal (3.3Vdc or 5Vdc dual voltage) PCI versions of the Intel Dialogic D/120JCT-LS and the D/120JCT-Euro cards, rather than the older single-bus voltage (5Vdc) versions of the cards.

Note that older Revision 1 LS cards are still supported for use with Cisco Unity version 4.0(x), but they cannot be ordered for new Cisco Unity version 4.0(x) installations. In addition, the older LS cards can be used only when they are appropriate for the available slots in the Cisco Unity server or expansion chassis.

If you are installing cards that have H.100 connectors, you need an H.100 cable that has at least as many connectors as you have cards (you must connect all cards by using a single cable) but no more than five extra connectors.

You may need to attach or remove the slot retainer bracket that ships with the card, depending on the mechanical configuration of the Cisco Unity server or expansion chassis.

Figure A-6 *D/120JCT-LS and D/120JCT-Euro Rev 1 (Conventional PCI) Top and Side Views*

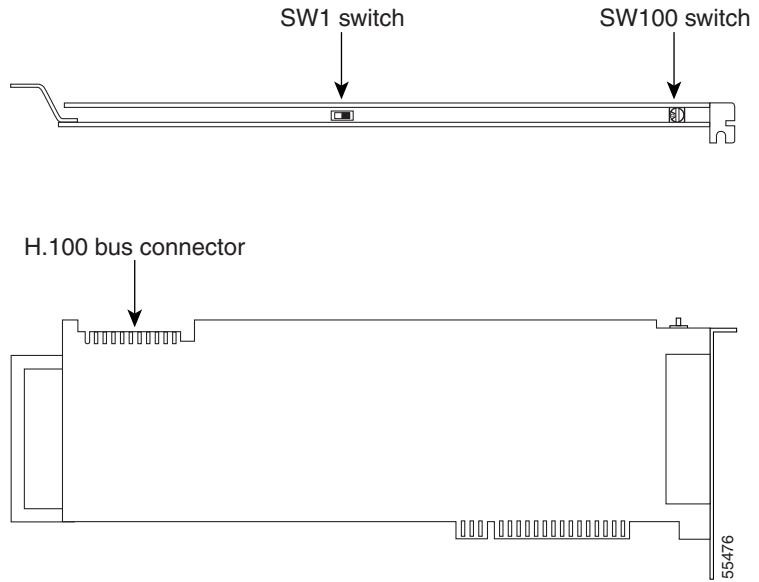


Figure A-7 *D/120JCT-LS and D/120JCT-Euro Rev 2 (uPCI) Top and Side Views*

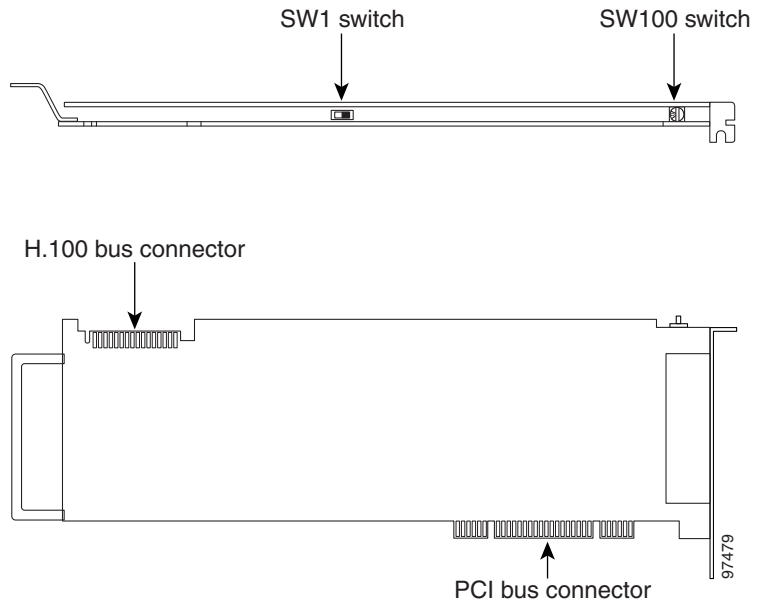
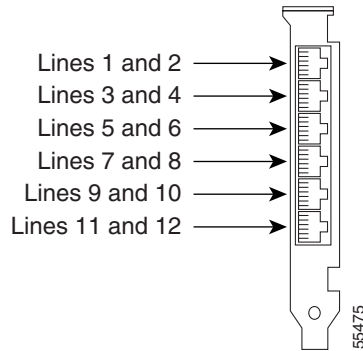
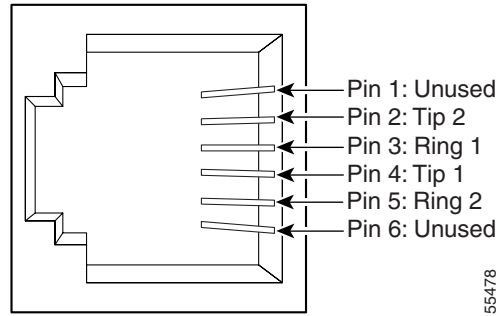


Figure A-8 D/120JCT-LS and D/120JCT-Euro Connection Pinouts and Backplate

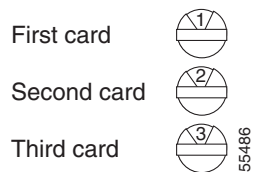


Hardware Settings

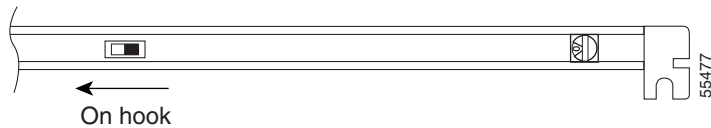
To Set the D/120JCT-LS and D/120JCT-Euro Card Switches

Step 1 Set the rotary switch (SW100) to a unique value for each card.

Each Intel Dialogic card in the Cisco Unity server or expansion chassis must have a unique value, starting with **1** and continuing in sequence on subsequent cards. For example, set the rotary switch on the first three voice cards as shown below. This is also the order in which you install the cards in the server.



- Step 2** Set the SW1 switch to **On Hook** on each card.



Software Settings

Do the following procedure only if the Cisco Unity server contains D/120JCT-Euro voice cards. There are no software settings for D/120JCT-LS voice cards.

To Select the Country for D/120JCT-Euro Voice Cards

- Step 1** Exit the Cisco Unity software, if it is running. For more information, see the [“Exiting and Starting the Cisco Unity Software and Server”](#) appendix.
- Step 2** Click **Programs > Administrative Tools > Services**.
- Step 3** In the right pane of the Services dialog box, right-click **Telephony**, and click **Stop**.
- Step 4** If you are prompted to stop other services, click **Yes**.
- Step 5** On the Windows Start menu, click **Programs > Dialogic System Software > Dialogic Configuration Manager–DCM**.
- Step 6** When the message “DCM could not detect devices...” appears, click **OK**.
- Step 7** In the DCM toolbar, click the red button to stop the Dialogic service.
- Step 8** When the Dialogic service has stopped, click **Close**.
- Step 9** In the Dialogic Configuration Manager dialog box, in the list of installed cards, double-click a D/120JCT-Euro card.
- Step 10** In the Dialogic Configuration Manager Properties dialog box, click the **Country** tab.
- Step 11** In the Country list, click the applicable value:

Euro (CTR-21)	For all countries that require CE conformity, including Austria, Belgium, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the United Kingdom.
Australia	For Australia.
New Zealand	For New Zealand.

- Step 12** If you chose Australia or New Zealand in the Country list, then in the Frequency Resolution list, click **FREQRES_LOW**.
- Step 13** Click **OK**.
- Step 14** Repeat Steps 9 through 13 for each D/120JCT-Euro card installed in the system.

- Step 15** Close the DCM.
- Step 16** Restart the Cisco Unity server.
-

Intel Dialogic D/240PCI-T1

The Dialogic D/240PCI-T1 voice card provides one T1 span with 24 channels of voice processing in a single PCI slot. The card connects directly to a channel-service unit, digital-service unit, or to other phone-network terminating equipment by using an RJ-48C connector.

If you are installing cards that have H.100 connectors, you need an H.100 cable that has at least as many connectors as you have cards (you must connect all cards by using a single cable) but no more than five extra connectors.

Figure A-9 D/240PCI-T1 Top and Side Views

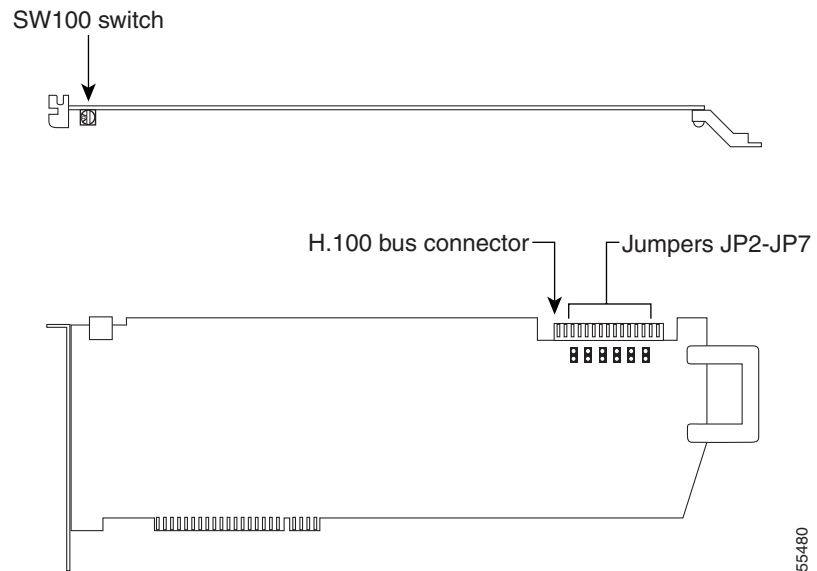
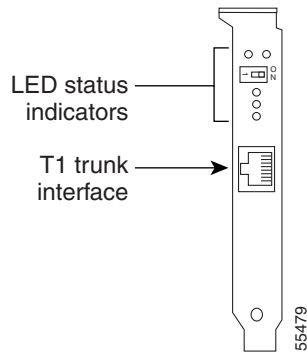
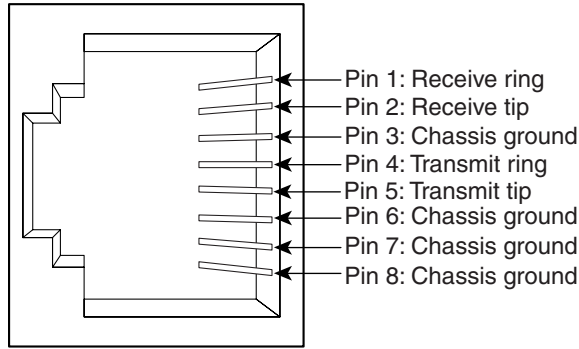


Figure A-10 D/240PCI-T1 Connection Pinouts and Backplate

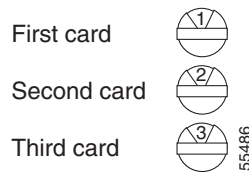


Hardware Settings

To Set the D/240PCI-T1 Card Switches and Jumpers

Step 1 Set the rotary switch (SW100) to a unique value.

Each Intel Dialogic card in the Cisco Unity server or expansion chassis must have a unique value, starting with **1** and continuing in sequence on subsequent cards. For example, set the rotary switch on the first three voice cards as shown below. This is also the order in which you install the cards in the server.



- Step 2** Settings for jumpers JP2 through JP5 depend on the number of D/240PCI-T1 voice cards in the Cisco Unity server:

One card	Set jumpers JP2 through JP5 to Off (Figure A-11) on the card.
Two cards	Set jumpers JP2 through JP5 to On (Figure A-12) on both cards.
Three or more cards	Set jumpers JP2 through JP5 to On (Figure A-12) on the first and last cards. Set jumpers JP2 through JP5 to Off (Figure A-11) on all other cards.

Figure A-11 D/240PCI-T1 Jumpers JP2 Through JP 5: Off

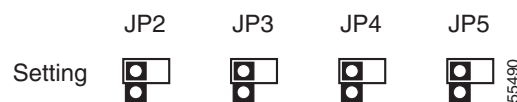
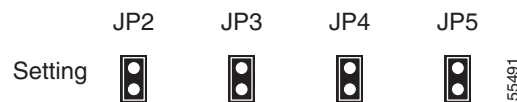
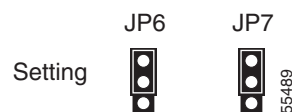


Figure A-12 D/240PCI-T1 Jumpers JP2 Through JP 5: On



- Step 3** On jumpers JP6 and JP7, install shunts on the top two pins (1 and 2).



Software Settings

For a D/240PCI-T1 voice card, set the protocol manually after the Cisco Unity Setup program is finished.

To Set the D/240PCI-T1 Protocol

- Step 1** On the Windows Start menu, click **Settings > Control Panel > Phone and Modem Options**.
- Step 2** In the Phone and Modem Options dialog box, click the **Advanced** tab.
- Step 3** Click **Dialogic Generation 2 Service Provider for NT**.
- Step 4** Click **Configure**.
- Step 5** In the Dialogic TSP Configuration dialog box, click **Advanced**.
- Step 6** In the Configuration Service dialog box, click the **Digital Protocols** tab.
- Step 7** In the Currently Assigned Protocols list, click **DtiB1 Undefined Protocol**.

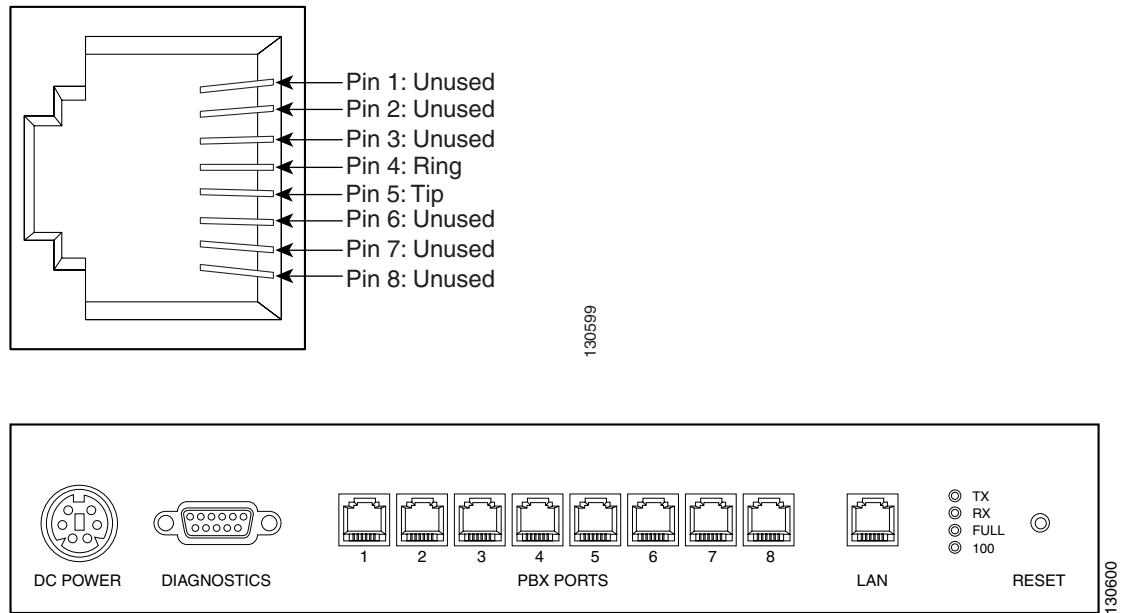
- Step 8** In the Available Protocols list, click **Us_Is_fxs_io**.
- Step 9** Click **Set Protocol**. DtiB1 Undefined Protocol changes to Us_Is_fxs_io.
- Step 10** If the Currently Assigned Protocols list contains more than one item (when the Cisco Unity server contains more than one D/240PCI-T1 card), repeat Steps 7 through 9 to change the remaining items from DtiB1 Undefined Protocol to Us_Is_fxs_io.
- Step 11** Click **OK** to close the Configuration Service dialog box.
- Step 12** Click **OK** to close the Dialogic TSP Configuration dialog box.
- Step 13** Click **Close** to close the Phone and Modem Options dialog box.
- Step 14** Close Control Panel.

Intel NetStructure PBX-IP Media Gateway (PIMG)

The Intel NetStructure PBX-IP Media Gateway (PIMG) units each connect to eight ports from a circuit-switched phone system (either analog or digital phone lines, depending on the model of the PIMG unit). The PIMG units communicate with the Cisco Unity server through the LAN by using Session Initiation Protocol (SIP).

The lines from the phone system attach to a PIMG unit with RJ-45 connectors, though it is possible to use RJ-11 connectors on these lines instead.

Figure A-13 PIMG Unit Connection Pinout and Port Connections



We recommend that the lines connect to the ports on the PIMG units in the same order as the ports on the phone system. For example, the first phone system port connects to the first port on the PIMG unit, the second phone system port connects to the second port on the PIMG unit, and so on.

Software Settings

Instructions for configuring PIMG units for integrating a phone system with Cisco Unity are found in the applicable Cisco Unity integration guide, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Removing Intel Dialogic Voice Card Software

Determining the Current Settings for the Quiet Parameter and Other Parameters

When the quiet parameter and any other parameters have been set to a value other than the default, the settings will be lost when you remove the Intel Dialogic software. Write down the current values of the parameters so you can restore the values after you reinstall the software. If the parameter-file value is blank, the Intel Dialogic default settings are being used, and you do not need to reset any parameter values when you reinstall the software.

To Determine the Current Settings for the Quiet Parameter and Other Parameters

-
- Step 1** Exit the Cisco Unity software, if it is running. For more information, see the “[Exiting the Cisco Unity Software](#)” section on page B-1.
 - Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 3** In the right pane of the Services dialog box, right-click **Telephony**, and click **Stop**.
 - Step 4** If you are prompted to stop other services, click **Yes**.
 - Step 5** On the Windows Start menu, click **Programs > Dialogic System Software > Dialogic Configuration Manager-DCM**.
The tree-structured list contains an entry for each Intel Dialogic card installed in the server.
 - Step 6** On the Service menu, click **Stop Service**.
 - Step 7** Double-click a card in the tree list.
 - Step 8** In the Properties dialog box for the card, click the **Misc** tab.
 - Step 9** In the Parameter list, click **ParameterFile**.
 - Step 10** Write down all the values in the Value field. You will re-enter the values later when you reset the parameters. Use the format <parameter name><XX>.prm.
If the Value field is blank, the Intel Dialogic default settings are being used.
 - Step 11** Click **OK**.
 - Step 12** Repeat [Step 7](#) through [Step 11](#) for any additional cards in the tree list.
-

Removing the Intel Dialogic Voice Card Software

The following procedure may differ slightly for earlier versions of Cisco Unity, which used an earlier version of Dialogic Configuration Manager.

To Remove Intel Dialogic Voice Card Software

-
- Step 1** Exit the Cisco Unity software, if it is running. For more information, see the [“Exiting the Cisco Unity Software”](#) section on page B-1.
 - Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 3** In the right pane of the Services dialog box, right-click **Telephony**, and click **Stop**.
 - Step 4** If you are prompted to stop other services, click **Yes**.
 - Step 5** On the Windows Start menu, click **Programs > Dialogic Systems Software > Dialogic Configuration Manager–DCM**.

Dialogic Configuration Manager may display an error message about not detecting devices. This error is harmless. Click **OK**.
 - Step 6** On the Service menu, click **Stop Service**.
 - Step 7** Click **Close**.
 - Step 8** Close the DCM.
 - Step 9** On the Windows Start menu, click **Settings > Control Panel > Phone and Modem Options**.
 - Step 10** Click the **Advanced** tab.
 - Step 11** Click **Dialogic Generation 2 Service Provider for NT** or **DSE Service Provider**, as applicable.
 - Step 12** Click **Remove**.
 - Step 13** Click **Yes**.
 - Step 14** Click **OK** to close the Phone and Modem Options dialog box.
 - Step 15** In Control Panel, double-click **Sounds and Multimedia**.
 - Step 16** In the Sounds and Multimedia Options dialog box, click the **Hardware** tab.
 - Step 17** Click **Legacy Audio Drivers**.
 - Step 18** Click **Properties**.
 - Step 19** In the Legacy Audio Drivers Properties dialog box, click the **Properties** tab.
 - Step 20** Expand **Audio Devices**.
 - Step 21** Click **Audio for Dialogic WAVE**.
 - Step 22** Click **Remove**.
 - Step 23** Click **Yes** to confirm.
 - Step 24** When prompted to restart the server, click **Don’t Restart Now**.



Caution If you restart now, the WAVE driver is not removed.

- Step 25** Click **OK** to close the Legacy Audio Drivers Properties dialog box.
- Step 26** Click **OK** to close the Sounds and Multimedia Properties dialog box.

- Step 27** Close Control Panel.
 - Step 28** On the Windows Start menu, click **Programs > Dialogic System Software > Uninstall**.
 - Step 29** Follow the on-screen prompts to uninstall the software.
If you are prompted to delete shared files, click **No to All**.
 - Step 30** Click **OK**.
 - Step 31** When the uninstallation is complete, click **Yes** to restart the server. (The Dialogic-triggered restart may not restart the session; in this case, manually restart.)
 - Step 32** After the server restarts, log on.
 - Step 33** In Windows Explorer, browse to the directory where Cisco Unity is installed (the default directory is CommServer), and delete the **Dialogic** directory.
-

Resetting the Quiet Parameter and Other Parameters

After you reinstall Intel Dialogic voice card software, do the following procedure to reset the quiet parameter to the value you identified in the [“Determining the Current Settings for the Quiet Parameter and Other Parameters”](#) section on page A-12.

To Reset the Quiet Parameter and Other Parameters

- Step 1** Exit the Cisco Unity software, if it is running. For more information, see the [“Exiting and Starting the Cisco Unity Software and Server”](#) appendix.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 3** In the right pane of the Services dialog box, right-click **Telephony**, and click **Stop**.
- Step 4** If you are prompted to stop other services, click **Yes**.
- Step 5** On the Windows Start menu, click **Programs > Dialogic System Software > Dialogic Configuration Manager–DCM**.
The tree-structured list contains an entry for each Intel Dialogic card installed in the server.
- Step 6** On the Service menu, click **Stop Service**.
- Step 7** Double-click a card in the tree list.
- Step 8** In the Properties dialog box for the card, click the **Misc** tab.
- Step 9** In the Parameter list, click **ParameterFile**.
- Step 10** In the Value field, enter all the values that you recorded in the earlier procedure and enter the quiet parameter last. Use the format **<parameter name><XX>.prm** followed by a **space**.
(For example, for the quiet parameter, enter quiet<XX>.prm, where XX = the -dBm level of the desired quiet parameter file. The recommended setting for Cisco Unity is 50.)
- Step 11** Click **OK**.

- Step 12** Repeat [Step 7](#) through [Step 11](#) for any additional cards in the tree list.
- Step 13** Restart the Cisco Unity server.
-



Exiting and Starting the Cisco Unity Software and Server

This appendix contains the following sections:

- [Exiting the Cisco Unity Software, page B-1](#)
- [Shutting Down or Restarting the Cisco Unity Server, page B-2](#)
- [Starting the Cisco Unity Software, page B-3](#)

Exiting the Cisco Unity Software

This section contains two procedures for exiting the Cisco Unity software: from the Cisco Unity server and from another computer.



Caution

Do not use `Kill av*.*` to exit the Cisco Unity software. `Kill av*.*` does not stop all Cisco Unity services, and may cause problems with upgrades from Cisco Unity version 2.x.

Do not stop `AvCsMgr` by using the Services window or the Component Services window as a method to exit the Cisco Unity software. Stopping the `AvCsMgr` does not stop all Cisco Unity services and may cause unexpected results.

To Exit the Cisco Unity Software from the Cisco Unity Server

- Step 1** If the system uses the automated attendant, route all calls to the operator.
- Step 2** On the Cisco Unity server, log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
- Step 3** Right-click the **Cisco Unity** icon in the status area of the taskbar.
(If the Cisco Unity icon is not in the taskbar, browse to the **CommServer** directory, and double-click `AvCsTrayStatus.exe`.)

- Step 4** Click **Stop Cisco Unity**.
- Step 5** Click **OK** to confirm that you want to exit the Cisco Unity software. Cisco Unity stops running when all calls are finished, and an “X” appears in the Cisco Unity icon.
- Step 6** Press **Ctrl-Alt-Delete**, then lock or log off of Windows to prevent access by unauthorized users.
-

To Exit the Cisco Unity Software from Another Computer

- Step 1** If the system uses the automated attendant, route all calls to the operator.
- Step 2** If the Cisco Unity Status Monitor does not use Integrated Windows authentication, skip to [Step 3](#).
When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
 - c. If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the administration account or the Windows domain account.
 - d. Skip to [Step 5](#).
- Step 3** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using any domain account that has the right to log on locally.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 4** On the Cisco Unity Log On page, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account, and click **Log On**.
- Step 5** In the Cisco Unity Status Monitor, under Shutting Down Cisco Unity, choose a method:
- Cisco Unity stops running after all calls are finished.
 - Cisco Unity interrupts calls in progress with a voice message, disconnects all calls, then stops running.
- Step 6** Click **Shut Down**.
-

Shutting Down or Restarting the Cisco Unity Server



Note

Restarting the Cisco Unity server may result in delayed message notification and message waiting indication until MAPI logon to all subscriber mailboxes has been completed. Depending on the size of the subscriber database, it could take several hours to complete the MAPI logon.

If the Cisco Unity system has an expansion chassis or is set up for failover, note the following considerations before shutting down or restarting the Cisco Unity server:

Expansion chassis connected to the Cisco Unity server	When both the expansion chassis and the Cisco Unity server are turned off, turn on the expansion chassis before you turn on the server. Otherwise, the server may not detect the voice cards in the expansion chassis.
Cisco Unity failover	<ul style="list-style-type: none"> • When both servers are running and the active server is shut down, the inactive server becomes active. • When neither server is running, the first server started becomes the active server. • When the secondary Cisco Unity server is active and configured for automatic failback, and the primary Cisco Unity server is also running, the secondary server attempts failback on the failback schedule.

To Shut Down or Restart the Cisco Unity Server

Step 1 Exit the Cisco Unity software, if it is running, by using one of the procedures in the [“Exiting the Cisco Unity Software”](#) section on page B-1.

Step 2 On the Windows Start menu, click **Shut Down**.

Step 3 Click **Shut Down** or **Restart**. During a restart, the Cisco Unity software starts automatically.

When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon in the status area of the taskbar.

When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon in the status area of the taskbar.

Starting the Cisco Unity Software

This section contains two procedures for starting the Cisco Unity software: from the Cisco Unity server and from another computer.

Cisco Unity is a Windows service that is configured to start automatically when you turn on or restart the server. Do one of the procedures in this section only if you exited the Cisco Unity software and did not restart the server.

Exchange must be running before you start the Cisco Unity software—either on the partner Exchange server or on the Cisco Unity server, depending on your configuration.

If Exchange stops for any reason while Cisco Unity is running, Cisco Unity will continue to take messages.

To Start the Cisco Unity Software from the Cisco Unity Server

- Step 1** On the Cisco Unity server, log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
- Step 2** Right-click the **Cisco Unity** icon in the status area of the taskbar.
(If the Cisco Unity icon is not in the taskbar, browse to the **CommServer** directory, and double-click **AvCsTrayStatus.exe**.)
- Step 3** Click **Start Cisco Unity**.
When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon.
When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon.
- Step 4** Press **Ctrl-Alt-Delete**, then lock or log off of Windows to prevent access by unauthorized users.
- Step 5** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.
-

To Start the Cisco Unity Software from Another Computer

- Step 1** If the Cisco Unity Status Monitor does not use Integrated Windows authentication, skip to [Step 2](#).
When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
 - c. If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account.
 - d. Skip to [Step 4](#).
- Step 2** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using any domain account that has the right to log on locally.
 - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 3** On the Cisco Unity Log On page, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account, and click **Log On**.
- Step 4** In the Cisco Unity Status Monitor, click the **System Status** icon (the first icon), at the top of the page.
- Step 5** Click **Start**.
- Step 6** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.
-



Manual Installation Procedures for Software Installed by the Cisco Unity System Preparation Assistant During a New Installation

This appendix contains procedures for manually installing the required Windows components, browser, database, and service packs that are automatically installed by the Cisco Unity System Preparation Assistant during a new installation. Install the components in the order listed.

This appendix contains the following sections:

- [Installing MSXML 3.0 with Service Pack 1, page C-1](#)
- [Installing Windows Terminal Services, page C-2](#)
- [Installing the NNTP Service, page C-2](#)
- [Installing Message Queuing Services 2.0, page C-2](#)
- [Installing Windows 2000 Service Pack 4, page C-3](#)
- [Installing Internet Explorer 6.0 with Service Pack 1, page C-3](#)
- [Installing SQL Server 2000 and Service Pack 3a, page C-4](#)
- [Installing the Microsoft .NET Framework, page C-5](#)

For more information about the Cisco Unity System Preparation Assistant, see the [“Running the Cisco Unity System Preparation Assistant”](#) section on page 5-6.

Installing MSXML 3.0 with Service Pack 1



Note

You are not required to install MSXML 3.0 before you install MSXML 3.0 Service Pack 1. MSXML 3.0 Service Pack 1 overwrites MSXML 3.0 if MSXML 3.0 is installed on the computer.

To Install MSXML 3.0 with Service Pack 1

- Step 1** On Cisco Unity Service Packs CD 1, browse to the **MSXML3_SP1** directory, and double-click **Mxml3sp1.exe**.
- Step 2** Follow the on-screen prompts to complete the installation.

Installing Windows Terminal Services

To Install Windows Terminal Services

- Step 1** On the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
 - Step 2** Click **Add/Remove Windows Components**.
 - Step 3** In the Windows Components dialog box, check the **Windows Terminal Services** check box. Do not change any other items.
 - Step 4** Click **Next**.
 - Step 5** In the Terminal Services Setup dialog box, click **Remote Administration Mode**, and click **Next**.
 - Step 6** When you are prompted, insert the Windows 2000 Server disc in the CD-ROM drive, and click **OK**. If the Cisco Unity server was purchased from Cisco, the disc is labeled “Cisco Unity System Disc.”
 - Step 7** In the Completing the Windows Components Wizard dialog box, click **Finish**.
 - Step 8** Click **Yes** to restart the server.
-

Installing the NNTP Service

To Install the NNTP Service

- Step 1** On the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
 - Step 2** Click **Add/Remove Windows Components**.
 - Step 3** Click **Internet Information Services (IIS)** (but do not uncheck the check box), and click **Details**.
 - Step 4** In the Internet Information Services (IIS) dialog box, check the **NNTP Service** check box. If the **SMTP Service** check box is not already checked, check it, too.
 - Step 5** Click **OK**.
 - Step 6** Click **Next**.
 - Step 7** When the installation is complete, click **Finish**.
 - Step 8** Close the Add/Remove Programs dialog box and Control Panel.
-

Installing Message Queuing Services 2.0

To Install Message Queuing Services 2.0

- Step 1** On the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
- Step 2** Click **Add/Remove Windows Components**.

- Step 3** In the Windows Components dialog box, check the **Message Queuing Services** check box. Do not change any other items.
- Step 4** Click **Next**.
- Step 5** In the Message Queuing Type dialog box, click **Next**. Do not change any items.
- Step 6** If the Message Queuing Server dialog box appears, click **Message Queuing Will Not Access a Directory Service**, and click **Next**.
- Step 7** If the Windows NT 4.0 Message Queuing Clients dialog box appears, click **No, Do Not Change the Permissions**, and click **Next**.
- Step 8** When you are prompted, insert the Windows 2000 Server disc in the CD-ROM drive, and click **OK**. If the Cisco Unity server was purchased from Cisco, the disc is labeled “Cisco Unity System Disc.”
- Step 9** In the Completing the Windows Components Wizard dialog box, click **Finish**.
- Step 10** Close the Add Remove Programs dialog box and Control Panel.
-

Installing Windows 2000 Service Pack 4

To Install Windows 2000 Service Pack 4

- Step 1** On Cisco Unity Service Packs CD 1, browse to the **Win2K_SP4\i386\Update** directory, and double-click **Update.exe**.
- Step 2** Follow the on-screen prompts to complete the installation.
- Step 3** Remove the disc, if applicable.
- Step 4** Restart the server.
-

Installing Internet Explorer 6.0 with Service Pack 1



Caution

When you install Internet Explorer, the file WScript.exe is installed automatically. Do not remove WScript.exe, or the Cisco Unity Setup program will fail.

To Install Internet Explorer 6.0 with Service Pack 1

- Step 1** On Cisco Unity Service Packs CD 1, browse to the **IE6SP1** directory, and double-click **IE6Setup.exe**.
- Step 2** Follow the on-screen prompts.
-

Installing SQL Server 2000 and Service Pack 3a

You install SQL Server 2000 on the primary and secondary Cisco Unity servers.

Do the following two procedures in the order listed.



Note

Install the application in the location you made note of in the [“Determining the Drive Locations for Files on the Cisco Unity Server”](#) section on page 2-4.

To Install SQL Server 2000

-
- Step 1** Log on to Windows.
 - Step 2** Insert the Cisco Unity Data Store 2000 disc in the CD-ROM drive.
 - Step 3** When the Microsoft SQL Server 2000 Standard Edition window appears, click **SQL Server 2000 Components**.
 - Step 4** In the Install Components window, click **Install Database Server**.
 - Step 5** In the Welcome dialog box, click **Next**.
 - Step 6** In the Computer Name dialog box, click **Next** to accept the default setting **Local Computer**.
 - Step 7** In the Installation Selection dialog box, click **Next** to accept the default setting **Create a New Instance of SQL Server, or Install Client Tools**.
 - Step 8** Follow the on-screen prompts until the CD Key dialog box appears.
 - Step 9** Enter the key for Cisco Unity Data Store 2000 from the sticker located on the CD sleeve, and click **Next**.
 - Step 10** In the Installation Definition dialog box, click **Next** to accept the default setting **Server and Client Tools**.
 - Step 11** In the Instance Name dialog box, check the **Default** check box.
 - Step 12** Click **Next**.
 - Step 13** In the Setup Type dialog box, click **Next** to accept the default setting **Typical**.
 - Step 14** At the top of the Services Accounts dialog box, click **Use the Same Account for Each Service**.
 - Step 15** Under Service Settings, click **Use the Local System Account**.



Note

You reset the accounts that SQL Server services log on as later. The Cisco Unity installation guide alerts you when to do the procedure later in the installation.

-
- Step 16** Click **Next**.
 - Step 17** In the Authentication Mode dialog box, we recommend that you click **Windows Authentication Mode**.
If you click **Mixed Mode** (which is supported, but less secure), under Add Password for the SA Login, enter and confirm a password for the SQL Server system administrator logon.
 - Step 18** Click **Next**.
 - Step 19** In the Start Copying Files dialog box, click **Next**.
 - Step 20** In the Choose Licensing Mode dialog box, click **Processor License For**, and specify the number of processors in the Cisco Unity server.
 - Step 21** Click **Continue**.

- Step 22** If you are prompted about shutdown tasks before continuing with the installation, click **Next**.
 - Step 23** Click **Finish**.
 - Step 24** Restart the server.
-

To Install SQL Server 2000 Service Pack 3a

- Step 1** On Cisco Unity Service Packs CD 1, browse to the **SQL2000_SP3\X86\Setup** directory, and double-click **Setupsql.exe**.
 - Step 2** On the Welcome screen, click **Next**.
 - Step 3** Follow the on-screen prompts until the Connect to Server dialog box appears.
 - Step 4** Select Windows authentication, and click **Next**.
 - Step 5** If the SA Password Warning dialog box appears, enter and confirm the password, and click **OK**.
 - Step 6** Check the **Upgrade Microsoft Search and Apply SQL Server 2000 SP3 (Required)** check box, and click **Continue**. (Do not check the Enable Cross-database Ownership Chaining for all Databases (Not Recommended) check box.)
 - Step 7** Follow the on-screen prompts.
 - Step 8** Click **Finish** to begin installing components.
 - Step 9** When the Setup message appears, click **OK**.
 - Step 10** Click **Finish** to restart the server.
-

Installing the Microsoft .NET Framework

To Install the Microsoft .NET Framework

- Step 1** On Cisco Unity Service Packs CD 1, browse to the **DotNet** directory, and double-click **Dotnetfx.exe**.
 - Step 2** Follow the on-screen prompts.
-

■ Installing the Microsoft .NET Framework



A

- accounts
 - administration [7-2](#)
 - creating for the Cisco Unity installation [7-3](#)
 - directory services [7-2](#)
 - installation [7-2](#)
 - local services [7-2](#)
 - message store services [7-2](#)
 - required for the Cisco Unity installation [7-2](#)
 - resetting account that SQL Server 2000 services log on as [5-14](#)
 - setting Exchange permissions for [7-8](#)
 - setting rights and permissions for [7-4](#)
- Active Directory
 - extending schema for Cisco Unity [6-6](#)
- adding
 - administration account to local Administrators group [7-3](#)
 - Cisco Unity server to existing domain [5-13](#)
- administration account
 - adding to local Administrators group [7-3](#)
 - creating [7-3](#)
 - description [7-2](#)
- Anonymous authentication
 - advantages and disadvantages of [10-2](#)
 - how it works with Cisco Unity Administrator [10-4](#)
 - using with Cisco Unity Administrator [10-2](#)
- assigning IP address [5-11](#)
- attaching peripheral devices to Cisco Unity server [3-5](#)
- authentication, methods available for Cisco Unity Administrator [10-2](#)

B

- browser, installing with Cisco Unity System Preparation Assistant [5-6](#)

C

- challenge/response authentication [10-2](#)
- changing folder settings in Windows Explorer [5-8](#)
- Cisco Security Agent for Cisco Unity
 - disabling service [5-12](#)
 - downloading [2-3](#)
 - installing [5-11](#)
 - re-enabling service [8-21](#)
- Cisco Unity
 - exiting software [B-1](#)
 - starting software [B-3](#)
- Cisco Unity Administrator
 - authentication methods available [10-2](#)
 - description [10-1](#)
 - setting up to use SSL [8-17](#)
- Cisco Unity Installation and Configuration Assistant
 - configuring Cisco Unity for message store [8-8](#)
 - configuring services [8-7](#)
 - description [8-3](#)
 - installing Cisco Unity software [8-4](#)
 - installing license files [8-6](#)
 - integrating phone system with Cisco Unity [8-10](#)
 - setting default passwords [8-9](#)
 - setting up the Cisco PCA to use SSL [8-10](#)
- Cisco Unity Install License File wizard, running [8-6](#)
- Cisco Unity Message Store Configuration wizard, running [8-8](#)
- Cisco Unity Permissions wizard, running [7-4](#)

Cisco Unity server

- adding to existing domain [5-13](#)
- attaching peripheral devices to [3-5](#)
- connecting phone system to [3-5](#)
- physical location of [3-5](#)
- restarting [B-2](#)
- securing [8-21](#)
- shutting down [B-2](#)

Cisco Unity Services Configuration wizard, running [8-7](#)

Cisco Unity software

- downloading for installation [2-2, 2-4](#)
- exiting [B-1](#)
- installing [8-4](#)
- registering [5-4](#)

Cisco Unity System Preparation Assistant [5-6](#)

- manual procedures for software installed by [C-1](#)

Cisco Unity Telephony Integration Manager,
running [8-10](#)

configuring

- Cisco Unity for message store [8-8](#)
- Cisco Unity services [8-7](#)
- Cisco Unity software [8-3](#)
- dual NIC in Cisco Unity server [5-2](#)
- IIS so Cisco Unity Administrator and Status Monitor use
Anonymous authentication [10-5](#)
- pcAnywhere [9-2](#)
- RAID arrays [4-1](#)
- TCP/IP properties [5-11](#)

connecting

- peripheral devices to Cisco Unity server [3-5](#)
- phone system [3-5](#)

conventions, documentation [ix](#)

creating

- accounts for the Cisco Unity installation [7-3](#)
- organizational units and mailbox store [6-7](#)

DD/120JCT-Euro [A-4](#)D/120JCT-LS [A-4](#)D/240PCI-T1 [A-8](#)D/41EPCI [A-1](#)D/41JCT-Euro [A-1](#)D/41JCT-LS [A-1](#)databases, SQL Server 2000, moving [8-18](#)data store software, installing manually [C-4](#)demonstration system, default license file for [5-6](#)Dialogic. *See* voice cards

directory and message store services account

creating [7-3](#)

directory services account

creating [7-3](#)description [7-2](#)setting Exchange permissions for [7-8](#)setting rights and permissions with Cisco Unity
Permissions wizard [7-4](#)

disabling

Cisco Security Agent service [5-12](#)Found New Hardware wizard for voice cards [5-10](#)virus-scanning services [5-12](#)

documentation

audience and use [ix](#)conventions [ix](#)required for the Cisco Unity installation [2-1](#)

domain

accounts required for the Cisco Unity installation [7-2](#)adding Cisco Unity server to existing [5-13](#)downloading software for installation [2-2](#)drive locations for files, determining [2-4](#)drivers-missing error message [3-1](#)dual NIC, configuring [5-2](#)**E**enabling Windows Terminal Services (Windows Server
2003 only) [4-9](#)error message, unknown PCI device [3-1](#)

Example Administrator account, securing against toll fraud [8-18](#)

Exchange

determining the partner server [6-2](#)

installing 2000 administration software on the Cisco Unity server [6-4](#)

installing 2003 administration software on the Cisco Unity server [6-2](#)

excluding from virus scanning directory in which Cisco Unity is installed [8-16](#)

exiting Cisco Unity software [B-1](#)

extending Active Directory schema for Cisco Unity [6-6](#)

F

files, drive locations for [2-4](#)

folder settings, changing in Windows Explorer [5-8](#)

Found New Hardware wizard, disabling for voice cards [5-10](#)

H

hardening Cisco Unity server [8-21](#)

I

IIS, configuring so Cisco Unity Administrator and Status Monitor use Anonymous authentication [10-5](#)

installation

accounts required for [7-2](#)

overview of mandatory tasks [1-1](#)

required documentation for [2-1](#)

installation account

creating [7-3](#)

description [7-2](#)

setting Exchange permissions for [7-8](#)

installing

browser with Cisco Unity System Preparation Assistant [5-6](#)

Cisco Security Agent for Cisco Unity [5-11](#)

Cisco Unity service release [8-16](#)

Cisco Unity software [8-4](#)

data store software, manually [C-4](#)

Exchange 2000 administration software on the Cisco Unity server [6-4](#)

Exchange 2003 administration software on the Cisco Unity server [6-2](#)

Internet Explorer 6.0 with Service Pack 1, manually [C-3](#)

latest service pack and updates for Exchange [6-5](#)

latest service packs and updates for Windows, Internet Explorer, and SQL Server 2000 [5-9](#)

license files [8-6](#)

Message Queuing Services, manually [C-2](#)

Microsoft .NET Framework, manually [C-5](#)

Microsoft Certificate Services component [8-3](#)

MSXML 3.0 with Service Pack 1, manually [C-1](#)

NIC-configuration utility [5-3](#)

NNTP Service, manually [C-2](#)

optional software [9-3](#)

pcAnywhere [9-1](#)

RSA SecurID [9-1](#)

service packs and updates with Cisco Unity System Preparation Assistant [5-6](#)

SQL Server 2000, manually [C-4](#)

SQL Server with Cisco Unity System Preparation Assistant [5-6](#)

virus-scanning software [5-10](#)

voice cards [3-1](#)

Windows 2000 Server [4-4](#)

Windows 2000 Service Pack 4, manually [C-3](#)

Windows components with Cisco Unity System Preparation Assistant [5-6](#)

Windows Server 2003 [4-3](#)

Windows Terminal Services, manually [C-2](#)

Integrated Windows authentication

advantages and disadvantages of [10-2](#)

how it works with Cisco Unity Administrator [10-3](#)

using with Cisco Unity Administrator [10-2](#)

integrating phone system with Cisco Unity [8-10](#)

Intel Dialogic. *See* voice cards

Intel NetStructure PBX-IP Media Gateway (PIMG) [A-11](#)

Internet Explorer 6.0 with Service Pack 1, installing manually [C-3](#)

IP address

assigning [5-11](#)

verifying [5-12](#)

J

jumpers and switches

D/240PCI-T1 [A-9](#)

D/41EPCI [A-2](#)

D/41JCT-LS and D/41JCT-Euro [A-4](#)

L

license files

default for Cisco Unity demonstration system [5-6](#)

getting a replacement copy [5-5](#)

installing [8-6](#)

obtaining [5-4](#)

local services account [7-2](#)

logical drives, setting up [4-10](#)

logs

SQL Server 2000, moving [8-18](#)

M

MAC address of Cisco Unity server [5-4](#)

mailbox store, creating [6-7](#)

manual procedures for software installed by Cisco Unity System Preparation Assistant [C-1](#)

Message Queuing Services, installing manually [C-2](#)

message store, configuring Cisco Unity for [8-8](#)

message store services account

creating [7-3](#)

description [7-2](#)

setting Exchange permissions for [7-8](#)

setting rights and permissions with Cisco Unity Permissions wizard [7-4](#)

Microsoft .NET Framework, installing manually [C-5](#)

Microsoft Certificate Services component, installing [8-3](#)

missing-drivers error message [3-1](#)

moving

SQL Server 2000 databases and transaction logs [8-18](#)

MSSQLServer service, resetting logon account [5-14](#)

MSXML 3.0 with Service Pack 1, installing manually [C-1](#)

N

network

securing Cisco Unity server [8-21](#)

verifying connection [5-12](#)

network interface card. *See* NIC [5-2](#)

NIC

configuration utility, installing [5-3](#)

configuring dual [5-2](#)

NNTP Service, installing manually [C-2](#)

non-universal PCI cards, slot placement [3-1](#)

NTLM authentication [10-2](#)

O

obtaining license files [5-4](#)

optional software, installing [9-3](#)

organizational units, creating [6-7](#)

P

PAK, location of [5-4](#)

partner Exchange server, determining [6-2](#)

Password Hardening wizard, running [8-9](#)

passwords

changing for the Example Administrator account [8-18](#)

setting default [8-9](#)

PBX-IP Media Gateway (PIMG) [A-11](#)

pcAnywhere
 installing [9-1](#)
 recommended configuration for [9-2](#)

peripheral devices, attaching [3-5](#)

permissions
 manually setting Exchange [7-8](#)
 setting with Cisco Unity Permissions wizard [7-4](#)

Permissions wizard, running [7-4](#)

phone system
 integrating with Cisco Unity and testing integration [8-10](#)
 making connections from [3-5](#)

PIMG units [A-11](#)
 connecting phone system to [3-5](#)

Platform Configuration discs
 utility for configuring RAID arrays [4-2](#)
 utility to install Windows 2000 Server [4-5](#)

product authorization key, location of [5-4](#)

Q

quiet parameter
 determining Intel Dialogic [A-12](#)
 resetting Intel Dialogic [A-14](#)

R

RAID arrays
 configuring [4-1](#)
 utilities on server manufacturer disc [4-3](#)
 utility on Platform Configuration discs [4-2](#)

re-enabling
 Cisco Security Agent service [8-21](#)
 virus-scanning services [8-21](#)

registering Cisco Unity software [5-4](#)

removing Intel Dialogic software [A-12](#)

resetting
 account that SQL Server 2000 services log on as [5-14](#)
 Intel Dialogic quiet parameter [A-14](#)

restarting Cisco Unity server [B-2](#)

rights, setting with Cisco Unity Permissions wizard [7-4](#)

RSA SecurID, installing [9-1](#)

S

schema, extending Active Directory for Cisco Unity [6-6](#)

securing
 Cisco Unity and the Cisco Unity server [8-21](#)
 Example Administrator account against toll fraud [8-18](#)

service packs
 downloading Cisco Unity CDs [2-4](#)
 downloading latest [2-3](#)
 installing latest for Exchange [6-5](#)
 installing latest for Windows, Internet Explorer, and SQL Server 2000 [5-9](#)
 installing with Cisco Unity System Preparation Assistant [5-6](#)

service release
 downloading [2-3](#)
 installing [8-16](#)

services, configuring Cisco Unity [8-7](#)

setting
 Exchange permissions, manually [7-8](#)
 rights and permissions with Cisco Unity Permissions wizard [7-4](#)

setting up
 Cisco Unity Administrator and Status Monitor to use SSL [8-17](#)
 logical drives [4-10](#)
 the Cisco PCA to use SSL [8-10](#)

Setup program, Cisco Unity [8-4](#)

shutting down Cisco Unity server [B-2](#)

software
 configuring for D/120JCT-Euro voice card [A-7](#)
 configuring for D/240PCI-T1 voice card [A-10](#)
 configuring for PIMG units [A-12](#)
 downloading for installation [2-2](#)
 exiting Cisco Unity [B-1](#)
 installing Cisco Unity [8-4](#)

- installing Exchange 2000 administration on the Cisco Unity server [6-4](#)
- installing Exchange 2003 administration on the Cisco Unity server [6-2](#)
- installing optional [9-3](#)
- registering Cisco Unity [5-4](#)
- removing Intel Dialogic [A-12](#)
- starting Cisco Unity [B-3](#)

SQL Server

- installing with Cisco Unity System Preparation Assistant [5-6](#)

SQL Server 2000

- installing manually [C-4](#)
- moving databases and transaction logs [8-18](#)
- resetting account that services log on as [5-14](#)

SQLServerAgent service, resetting logon account [5-14](#)

SSL

- determining whether to use [8-2](#)
- installing Microsoft Certificate Services component [8-3](#)
- setting up Cisco Unity Administrator and Status Monitor to use [8-17](#)
- setting up the Cisco PCA to use [8-10](#)

starting Cisco Unity software [B-3](#)

Status Monitor, setting up to use SSL [8-17](#)

switches and jumpers

- D/240PCI-T1 [A-9](#)
- D/41EPCI [A-2](#)
- D/41JCT-LS and D/41JCT-Euro [A-4](#)

T

- TCP/IP properties, configuring [5-11](#)
- toll fraud, preventing [8-18](#)
- transaction logs
 - moving SQL Server 2000 [8-18](#)

U

- UDDI Services, do not install [4-3](#)

- universal PCI voice cards, slot placement [3-1](#)
- unknown PCI device error message [3-1](#)
- updates
 - downloading latest [2-3](#)
 - installing latest for Exchange [6-5](#)
 - installing latest for Windows, Internet Explorer, and SQL Server 2000 [5-9](#)
- utilities
 - RAID array configuration, on disc from server manufacturer [4-3](#)
 - RAID array configuration, on Platform Configuration discs [4-2](#)
 - Windows 2000 Server installation, on disc from server manufacturer [4-7](#)
 - Windows 2000 Server installation, on Platform Configuration discs [4-5](#)
 - Windows Server 2003 installation, on disc from server manufacturer [4-4](#)
- UTIM. *See* Cisco Unity Telephony Integration Manager

V

- verifying IP address and network connection [5-12](#)
- virus scanning
 - disabling services [5-12](#)
 - excluding directory in which Cisco Unity is installed [8-16](#)
 - installing software [5-10](#)
 - re-enabling services [8-21](#)
- voice cards
 - D/120JCT-Euro [A-4](#)
 - D/120JCT-LS [A-4](#)
 - D/240PCI-T1 [A-8](#)
 - D/41EPCI [A-1](#)
 - D/41JCT-Euro [A-1](#)
 - D/41JCT-LS [A-1](#)
 - disabling Found New Hardware wizard for [5-10](#)
 - installing [3-1](#)
 - removing Intel Dialogic software [A-12](#)
 - slot placement [3-1](#)

W

Windows 2000 Server

installing [4-4](#)

Service Pack 4, installing manually [C-3](#)

Windows components, installing with Cisco Unity System
Preparation Assistant [5-6](#)

Windows Explorer, changing folder settings in [5-8](#)

Windows Server 2003

installing [4-3](#)

UDDI Services, do not install [4-3](#)

Windows Terminal Services, enabling (Windows Server
2003 only) [4-9](#)

Windows Terminal Services, installing manually [C-2](#)

